

# Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP2005/019938

International filing date: 25 October 2005 (25.10.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP  
Number: 2004-314723  
Filing date: 28 October 2004 (28.10.2004)

Date of receipt at the International Bureau: 28 November 2005 (28.11.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland  
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日  
Date of Application: 2004年10月28日

出 願 番 号  
Application Number: 特願2004-314723

パリ条約による外国への出願  
に用いる優先権の主張の基礎  
となる出願の国コードと出願  
番号

The country code and number  
of your priority application,  
to be used for filing abroad  
under the Paris Convention, is

J P 2004-314723

出 願 人  
Applicant(s): キヤノン株式会社

2005年11月 9日

特許庁長官  
Commissioner,  
Japan Patent Office

中 嶋



【書類名】	特許願
【整理番号】	0010014-01
【提出日】	平成16年10月28日
【あて先】	特許庁長官殿
【国際特許分類】	G06F 7/00
【発明者】	
【住所又は居所】	東京都大田区下丸子3丁目30番2号 キヤノン株式会社内
【氏名】	替地 修也
【特許出願人】	
【識別番号】	000001007
【氏名又は名称】	キヤノン株式会社
【代理人】	
【識別番号】	100076428
【弁理士】	
【氏名又は名称】	大塚 康徳
【電話番号】	03-5276-3241
【選任した代理人】	
【識別番号】	100112508
【弁理士】	
【氏名又は名称】	高柳 司郎
【電話番号】	03-5276-3241
【選任した代理人】	
【識別番号】	100115071
【弁理士】	
【氏名又は名称】	大塚 康弘
【電話番号】	03-5276-3241
【連絡先】	担当
【選任した代理人】	
【識別番号】	100116894
【弁理士】	
【氏名又は名称】	木村 秀二
【電話番号】	03-5276-3241
【手数料の表示】	
【予納台帳番号】	003458
【納付金額】	16,000円
【提出物件の目録】	
【物件名】	特許請求の範囲 1
【物件名】	明細書 1
【物件名】	図面 1
【物件名】	要約書 1
【包括委任状番号】	0102485

【書類名】 特許請求の範囲

【請求項 1】

可搬性の無線通信デバイスと通信するための無線通信手段を有し、受信した情報に基づいて所定の処理を実行する無線通信装置であって、

無線通信デバイスと通信を開始するため、認証処理の開始を指示する指示手段と、

該指示手段で認証開始が指示された場合、前記無線通信手段により、照合データを含む探索信号を発信する発信手段と、

該発信手段で前記探索信号を発信した後、前記無線通信手段によって唯一の無線通信デバイスから応答信号を受信し、当該応答信号中に前記照合データが含まれる場合、前記無線通信デバイスに認証情報を送信する認証手段と

を備えることを特徴とする無線通信装置。

【請求項 2】

可搬性の無線通信デバイスと通信するための無線通信手段を有し、受信した情報に基づいて所定の処理を実行する無線通信装置であって、

無線通信デバイスと通信を開始するため、認証処理の開始を指示する指示手段と、

該指示手段で認証開始が指示された場合、前記無線通信手段により、応答時間隔データを含む探索信号を発信する発信手段と、

該発信手段で前記探索信号を発信した後、前記無線通信手段によって唯一の無線通信デバイスから前記応答時間間隔で応答信号を受信した場合、前記無線通信デバイスに認証情報を送信する認証手段と

を備えることを特徴とする無線通信装置。

【請求項 3】

可搬性の無線通信デバイスと通信するための無線通信手段を有し、受信した情報に基づいて所定の処理を実行する無線通信装置であって、

前記無線通信手段で受信する信号強度を検出する検出手段と、

無線通信デバイスと通信を開始するため、認証処理の開始を指示する指示手段と、

該指示手段で認証開始が指示された場合、前記無線通信手段により、所定探索信号を発信する発信手段と、

該発信手段で前記探索信号を発信した後、前記無線通信手段によって唯一の無線通信デバイスから複数回の応答信号を受信し、且つ、各応答信号の受信強度差の絶対値が所定閾値  $T_1$  より大きく、所定閾値  $T_2$  未満 ( $T_2 > T_1 > 0$ ) の場合、前記無線通信デバイスに認証情報を送信する認証手段と

を備えることを特徴とする無線通信装置。

【請求項 4】

可搬性の無線通信デバイスと通信するための無線通信手段を有し、受信した情報に基づいて所定の処理を実行する無線通信装置であって、

無線通信デバイスと通信を開始するため、認証処理の開始を指示する指示手段と、

該指示手段で認証開始が指示された場合、前記無線通信手段に対し、認証後の通信可能エリアより狭い認証エリアに設定する設定手段と、

該設定手段で前記認証エリアに設定した後、前記無線通信手段により、所定探索信号を発信する発信手段と、

該発信手段で前記探索信号を発信した後、前記無線通信手段によって唯一の無線通信デバイスから応答信号を受信した場合、当該無線通信デバイスに認証情報を送信する認証手段と

を備えることを特徴とする無線通信装置。

【請求項 5】

可搬性の無線通信デバイスと通信し、所定の処理を実行する無線通信装置であって、

認証情報に基づく通常モードと、認当該通常モードよりも狭く、認証用のエリア範囲内で通信する認証モードとを切り換え可能な無線通信手段と、

前記無線通信手段で受信する信号強度を検出する検出手段と、

無線通信デバイスと通信を開始するため、認証処理の開始を指示する指示手段と、

該指示手段で認証開始が指示された場合、前記無線通信手段を前記認証モードに設定し、照合データ並びに応答時間間隔データを含む探索信号を発信する発信手段と、

該発信手段で前記探索信号を発信した後、前記無線通信手段によって、唯一の無線通信デバイスから前記応答時間間隔で、前記照合データを含む応答信号を受信し、且つ、前記検出手段で検出した各応答信号の受信強度差の絶対値が所定閾値 $T_1$ より大きく以上、所定閾値 $T_2$ 未満( $T_2 > T_1 > 0$ )の場合、前記無線通信デバイスに認証情報を送信する認証手段と

を備えることを特徴とする無線通信装置。

#### 【請求項6】

所定の無線通信装置と通信し、処理対象の情報を送信するための無線通信手段を備える電子機器であって、

前記無線通信装置と通信を開始するため、認証処理の開始を指示する指示手段と、

該指示手段で認証開始が指示された場合、探索信号を前記無線通信手段で受信する第1の受信手段と、

受信した探索情報中に含まれる照合データを含む応答信号を前記無線通信手段を介して送信する送信手段と、

該送信手段で送信した後、前記無線通信手段を介して認証情報を受信する第2の受信手段とを備え、

前記第2の受信手段で認証情報を受信した場合、これ以降は認証情報も基づいて前記無線通信装置と通信することを特徴とする電子機器。

#### 【請求項7】

所定の無線通信装置と通信し、処理対象の情報を送信するための無線通信手段を備える電子機器であって、

前記無線通信装置と通信を開始するため、認証処理の開始を指示する指示手段と、

該指示手段で認証開始が指示された場合、前記無線通信手段に対し、認証後の通信可能エリアより狭い認証エリアに設定する設定手段と、

該設定手段で前記認証エリアに設定した後、前記無線通信手段により、所定探索信号を受信する第1の受信手段と、

該第1の受信手段の受信に応じて応答信号を前記無線通信手段を介して送信する送信手段と、

該送信手段で送信した後、前記無線通信手段を介して認証情報を受信する第2の受信手段とを備え、

前記第2の受信手段で認証情報を受信した場合、これ以降は認証情報に基づいて前記無線通信装置と通信することを特徴とする電子機器。

#### 【請求項8】

所定の無線通信装置と通信し、処理対象の情報を送信するための無線通信手段を備える電子機器であって、

前記無線通信装置と通信を開始するため、認証処理の開始を指示する指示手段と、

該指示手段で認証開始が指示された場合、前記無線通信手段に対し、認証後の通信可能エリアより狭い認証エリアに設定する設定手段と、

該設定手段で前記認証エリアに設定した後、前記無線通信手段により、所定探索信号を受信する第1の受信手段と、

受信した探索情報中に含まれる照合データを含む応答信号を、前記無線通信手段を介して、前記探索情報に含まれる時間間隔の指示情報にしたがった時間間隔で送信する送信手段と、

該送信手段で送信した後、前記無線通信手段を介して認証情報を受信する第2の受信手段とを備え、

前記第2の受信手段で認証情報を受信した場合、これ以降は認証情報も基づいて前記無線通信装置と通信することを特徴とする電子機器。

【請求項 9】

可搬性の無線通信デバイスと通信するための無線通信手段を有し、受信した情報に基づいて所定の処理を実行する無線通信装置の制御方法であって、

無線通信デバイスと通信を開始するため、認証処理の開始を指示する指示工程と、

該指示工程で認証開始が指示された場合、前記無線通信手段により、照合データを含む探索信号を発信する発信工程と、

該発信工程で前記探索信号を発信した後、前記無線通信手段によって唯一の無線通信デバイスから応答信号を受信し、当該応答信号中に前記照合データが含まれる場合、前記無線通信デバイスに認証情報を送信する認証工程と

を備えることを特徴とする無線通信装置の制御方法。

【請求項 10】

可搬性の無線通信デバイスと通信するための無線通信手段を有し、受信した情報に基づいて所定の処理を実行する無線通信装置の制御方法であって、

無線通信デバイスと通信を開始するため、認証処理の開始を指示する指示工程と、

該指示工程で認証開始が指示された場合、前記無線通信手段により、応答時間隔データを含む探索信号を発信する発信工程と、

該発信工程で前記探索信号を発信した後、前記無線通信手段によって唯一の無線通信デバイスから前記応答時間間隔で応答信号を受信した場合、前記無線通信デバイスに認証情報を送信する認証工程と

を備えることを特徴とする無線通信装置の制御方法。

【請求項 11】

可搬性の無線通信デバイスと通信するための無線通信手段を有し、受信した情報に基づいて所定の処理を実行する無線通信装置の制御方法であって、

前記無線通信手段で受信する信号強度を検出する検出工程と、

無線通信デバイスと通信を開始するため、認証処理の開始を指示する指示工程と、

該指示工程で認証開始が指示された場合、前記無線通信手段により、所定探索信号を発信する発信工程と、

該発信工程で前記探索信号を発信した後、前記無線通信手段によって唯一の無線通信デバイスから複数回の応答信号を受信し、且つ、各応答信号の受信強度差の絶対値が所定閾値  $T_1$  より大きく、所定閾値  $T_2$  未満 ( $T_2 > T_1 > 0$ ) の場合、前記無線通信デバイスに認証情報を送信する認証工程と

を備えることを特徴とする無線通信装置の制御方法。

【請求項 12】

可搬性の無線通信デバイスと通信するための無線通信手段を有し、受信した情報に基づいて所定の処理を実行する無線通信装置の制御方法であって、

無線通信デバイスと通信を開始するため、認証処理の開始を指示する指示工程と、

該指示工程で認証開始が指示された場合、前記無線通信手段に対し、認証後の通信可能エリアより狭い認証エリアに設定する設定工程と、

該設定工程で前記認証エリアに設定した後、前記無線通信手段により、所定探索信号を発信する発信工程と、

該発信工程で前記探索信号を発信した後、前記無線通信手段によって唯一の無線通信デバイスから応答信号を受信した場合、当該無線通信デバイスに認証情報を送信する認証工程と

を備えることを特徴とする無線通信装置の制御方法。

【請求項 13】

可搬性の無線通信デバイスと通信し、所定の処理を実行する無線通信装置の制御方法であって、

所定の無線通信手段に対し、認証情報に基づく通常モードと、認当該通常モードよりも狭く、認証用のエリア範囲内で通信する認証モードとを切り換え可能な無線通信切り換え工程と、

前記無線通信手段で受信する信号強度を検出する検出工程と、

無線通信デバイスと通信を開始するため、認証処理の開始を指示する指示工程と、

該指示工程で認証開始が指示された場合、前記無線通信手段を前記認証モードに設定し、照合データ並びに応答時間間隔データを含む探索信号を発信する発信工程と、

該発信工程で前記探索信号を発信した後、前記無線通信手段によって、唯一の無線通信デバイスから前記応答時間間隔で、前記照合データを含む応答信号を受信し、且つ、前記検出工程で検出した各応答信号の受信強度差の絶対値が所定閾値 $T_1$ より大きく以上、所定閾値 $T_2$ 未満( $T_2 > T_1 > 0$ )の場合、前記無線通信デバイスに認証情報を送信する認証工程と

を備えることを特徴とする無線通信装置の制御方法。

#### 【請求項 14】

所定の無線通信装置と通信し、処理対象の情報を送信するための無線通信手段を備える電子機器の制御方法であって、

前記無線通信装置と通信を開始するため、認証処理の開始を指示する指示工程と、

該指示工程で認証開始が指示された場合、探索信号を前記無線通信手段で受信する第1の受信工程と、

受信した探索情報中に含まれる照合データを含む応答信号を前記無線通信手段を介して送信する送信工程と、

該送信工程で送信した後、前記無線通信手段を介して認証情報を受信する第2の受信工程とを備え、

前記第2の受信工程で認証情報を受信した場合、これ以降は認証情報も基づいて前記無線通信装置と通信することを特徴とする電子機器の制御方法。

#### 【請求項 15】

所定の無線通信装置と通信し、処理対象の情報を送信するための無線通信手段を備える電子機器の制御方法であって、

前記無線通信装置と通信を開始するため、認証処理の開始を指示する指示工程と、

該指示工程で認証開始が指示された場合、前記無線通信手段に対し、認証後の通信可能エリアより狭い認証エリアに設定する設定工程と、

該設定工程で前記認証エリアに設定した後、前記無線通信手段により、所定探索信号を受信する第1の受信工程と、

該第1の受信工程の受信に応じて応答信号を前記無線通信手段を介して送信する送信工程と、

該送信工程で送信した後、前記無線通信手段を介して認証情報を受信する第2の受信工程とを備え、

前記第2の受信工程で認証情報を受信した場合、これ以降は認証情報も基づいて前記無線通信装置と通信することを特徴とする電子機器の制御方法。

#### 【請求項 16】

所定の無線通信装置と通信し、処理対象の情報を送信するための無線通信手段を備える電子機器の制御方法であって、

前記無線通信装置と通信を開始するため、認証処理の開始を指示する指示工程と、

該指示工程で認証開始が指示された場合、前記無線通信手段に対し、認証後の通信可能エリアより狭い認証エリアに設定する設定工程と、

該設定工程で前記認証エリアに設定した後、前記無線通信手段により、所定探索信号を受信する第1の受信工程と、

受信した探索情報中に含まれる照合データを含む応答信号を、前記無線通信手段を介して、前記探索情報に含まれる時間間隔の指示情報にしたがった時間間隔で送信する送信工程と、

該送信工程で送信した後、前記無線通信手段を介して認証情報を受信する第2の受信工程とを備え、

前記第2の受信工程で認証情報を受信した場合、これ以降は認証情報も基づいて前記無

線通信装置と通信することを特徴とする電子機器の制御方法。

【請求項 17】

可搬性の無線通信デバイスと通信し、所定の処理を実行する無線通信装置用のコンピュータプログラムであって、

認証情報に基づく通常モードと、認当該通常モードよりも狭く、認証用のエリア範囲内で通信する認証モードとを切り換え可能な無線通信手段と、

前記無線通信手段で受信する信号強度を検出する検出手段と、

無線通信デバイスと通信を開始するため、認証処理の開始を指示する指示手段と、

該指示手段で認証開始が指示された場合、前記無線通信手段を前記認証モードに設定し、照合データ並びに応答時間間隔データを含む探索信号を発信する発信手段と、

該発信手段で前記探索信号を発信した後、前記無線通信手段によって、唯一の無線通信デバイスから前記応答時間間隔で、前記照合データを含む応答信号を受信し、且つ、前記検出手段で検出した各応答信号の受信強度差の絶対値が所定閾値  $T_1$  より大きく以上、所定閾値  $T_2$  未満 ( $T_2 > T_1 > 0$ ) の場合、前記無線通信デバイスに認証情報を送信する認証手段

として機能することを特徴とするコンピュータプログラム。

【請求項 18】

所定の無線通信装置と通信し、処理対象の情報を送信するための無線通信手段を備える電子機器用のコンピュータプログラムであって、

前記無線通信装置と通信を開始するため、認証処理の開始を指示する指示手段と、

該指示手段で認証開始が指示された場合、前記無線通信手段に対し、認証後の通信可能エリアより狭い認証エリアに設定する設定手段と、

該設定手段で前記認証エリアに設定した後、前記無線通信手段により、所定探索信号を受信する第 1 の受信手段と、

受信した探索情報中に含まれる照合データを含む応答信号を、前記無線通信手段を介して、前記探索情報に含まれる時間間隔の指示情報にしたがった時間間隔で送信する送信手段と、

該送信手段で送信した後、前記無線通信手段を介して認証情報を受信する第 2 の受信手段

として機能し、前記第 2 の受信手段で認証情報を受信した場合、これ以降は認証情報も基づいて前記無線通信装置と通信することを特徴とするコンピュータプログラム。

【請求項 19】

請求項 17 または請求項 18 に記載のコンピュータプログラムを格納したことを特徴とするコンピュータ可読記憶媒体。



【書類名】 明細書

【発明の名称】 無線通信装置の接続対象検出及び認証方法

【技術分野】

【0001】

本発明は無線通信装置間で通信パラメータ及びアドレス識別子等の認証情報を交換する際の、無線通信装置の接続対象検出及び認証方法に関するものである。

【背景技術】

【0002】

近年、携帯電話、PDA(Personal Digital Assistants)などの情報端末、パーソナルコンピュータ、及びプリンタに代表されるパーソナルコンピュータの周辺機器等、多種多様な情報機器のデータ通信や制御において、無線通信接続の利用が急増している。この無線通信接続の無線通信システムでは、公衆回線網だけに留まらず、Bluetooth(R)や、ワイヤレスLAN(Wireless LAN)等のローカルな回線も利用されている。

【0003】

前記した情報機器以外にも、デジタルカメラ等の撮像装置、家電製品、及びアクセサリ等、様々な機器に無線通信機能が搭載されつつあり、さらに有線通信接続方法として広く普及しているUSB(Universal Serial Bus)の無線化も進められている。

【0004】

無線通信装置で無線データ通信を行う際には、不特定の装置や意図しない装置と接続されないようにするために、認証という手続きをとることが多い。この認証に際しては、PIN(Personal Identification Number)コードやESSID(Extended Service Set Identifier)等を認証情報の一つとして無線通信装置間で交換し、認証情報交換した特定の2つの無線通信装置が、この認証情報で1対1の関連付けを行うことで、無線通信の認証セキュリティを確保している。

【0005】

この認証情報は、第三者に開示されてはならないものであり、この認証情報が第三者に漏洩した場合、この漏洩した認証情報を用いることによって、第三者が、装置内に格納されている書類、住所録、電子メール、個人情報、及び画像データ等にアクセスする恐れがある。また、無線通信システムや課金システム、プリントシステムが第三者によって不正利用される恐れもある。このような状況の中、これら無線通信装置のセキュリティ対策が注目されている。

【0006】

無線通信装置を相互に認証させる認証情報の入力方法は幾つかある。具体的には、使用者が手動で入力する方法、SIM(Subscriber Identify Module)カードを機器に挿入する方法、赤外線通信を利用して認証を行う方法、及び接続ケーブルを利用して認証を行う方法、装置内に二つの無線通信手段を持ち、片方の無線通信手段で認証を行う方法等がある。通信パラメータ及びアドレス識別子等の認証情報は、無線通信装置相互の認証が終了した後に、無線通信装置相互の記憶部に格納され、データ通信時には、格納された認証情報を用いて無線データ通信路の確保を行う。

【0007】

セキュリティ対策を行って無線通信装置の認証を行う方法としては、2つの通信装置の間で無線通信を行う場合に、第1の装置を第2の装置のドッキングポートに部分的に係合した時点で(第1の通信手段)、第1の装置と第2の装置が自動的に第2の通信手段により接続を行い、アドレス識別子交換を行う提案がある(特許文献1)。これによると、十分に近い範囲にない通信装置にはアドレス識別子及び暗号キーの開示は行われず、セキュリティの向上が期待できる。

【0008】

また、無線通信が可能な第1通信部と前記第1通信部とは異なる第2通信部とを有する第1通信機器と第2通信機器が、互いの第2通信部を接続すると2つの機器の間で無線通信を行うための通信パラメータを決定し、ユーザによる無線通信に必要な通信パラメータの設定を不要にする提案もある（特許文献2）。

【特許文献1】特許第3422683号公報

【特許文献2】特開2002-359623公報

【発明の開示】

【発明が解決しようとする課題】

【0009】

特定の2つの無線通信装置を関連付けする認証情報は、そのワード長がランダムで長いほどセキュリティの強度が高いが、使用者が手動で入力する場合は、使用者に面倒な操作をさせことになる。このため、使用者が手動で入力する認証情報は、ワード長が短く、第三者が推測しやすいコードとなることが多い。赤外線通信で認証を行う方法は、使用者に面倒な操作をさせることになり、狭すぎる指向性にも気を遣わせる不便がある。接続ケーブルで認証を行う方法も装置を互いに有線接続する必要があり、これも面倒である。

【0010】

また、前記従来例では、無線通信装置はデータ通信前に有線接続またはドッキングポートに結合しなければ、通信パラメータ及びアドレス識別子等の認証情報の交換が出来ないため、使用者に面倒な操作をさせるばかりでなく、認証処理と、データ通信とにおいて各々別の無線通信手段を用いなければならず、無線通信装置の簡素化、省電力化及び小型化の妨げとなっている。

【0011】

このように、無線通信装置の認証方法として、通信パラメータ及びアドレス識別子等の認証情報を簡便に設定し、使用者にとって使い勝手の良いシステム（無線通信システム、プリントシステム）を提供できていないという問題点があった。

【0012】

本発明は、操作者にかかる作業を簡便なものとし、且つ、単一の無線通信手段を利用しながらも、2つの無線通信装置間の認証処理を行える技術を提供しようとするものである。

【課題を解決するための手段】

【0013】

この課題を解決するため、例えば本発明の無線通信装置は以下の構成を備える。すなわち、

可搬性の無線通信デバイスと通信するための無線通信手段を有し、受信した情報に基づいて所定の処理を実行する無線通信装置であって、

無線通信デバイスと通信を開始するため、認証処理の開始を指示する指示手段と、

該指示手段で認証開始が指示された場合、前記無線通信手段により、照合データを含む探索信号を発信する発信手段と、

該発信手段で前記探索信号を発信した後、前記無線通信手段によって唯一の無線通信デバイスから応答信号を受信し、当該応答信号中に前記照合データが含まれる場合、前記無線通信デバイスに認証情報を送信する認証手段とを備える。

【発明の効果】

【0014】

本発明によれば、操作者にかかる作業を簡便なものとし、且つ、それぞれの装置が単一の無線通信手段を利用しながらも、二者間の認証処理を行えるようになる。

【発明を実施するための最良の形態】

【0015】

以下、添付図面に従って本発明に係る実施形態を詳細に説明する。

【0016】

図1は、本発明の実施の形態に係る無線通信ホスト装置であるプリンタ装置1（以下、

ホスト 1) のブロック構成図である。

【0017】

同図において、101はホスト1全体の制御を司るCPUであり、102はCPU101のワークエリアとして使用されるRAMである。103はCPU101の処理手順を記憶しているROMである。ただし、ROMは書き換えが可能な不揮発性メモリ、例えばフラッシュメモリで構成される。104は画像処理部であり、デジタル画像データ等をプリント可能なデジタルデータに変換するのに用いられる。105は各種表示を行うための表示制御部である。106は液晶表示器であり、デジタル画像データの確認や各種設定を行う際のメニューを表示するために使用される。107は発光ダイオードであり、ホスト1の処理状態を示すインジケータとして使用される。108は外部記憶装置の制御部であり、メモリソケット109に挿入されたコンパクトフラッシュ（登録商標）やメモリースティック（登録商標）等の記憶媒体に記憶されているデジタルデータの読み込み及び、記憶媒体へのデジタルデータの書き出しの制御を行う。110はUSBインターフェースの制御部であり、USBコネクタ111で他のUSBインターフェースを持つ装置と接続される。112は暗号処理部であり、認証情報や無線データ通信の暗号化を行うために使用される。113はリアルタイムクロックであり、認証期間カウントやアクセス時間記録を行うために使用される。120は無線通信を行うための無線通信部、121は無線通信を行うためのアンテナである。114は各種操作を行うボタン等の制御部であり、操作キー115、認証処理開始を指示する操作ボタン116、リセットボタン117の操作情報をCPU101へ伝えるために使用される。118はホスト1のプリンタ機能の制御部であり、プリンタエンジン119でデジタルデータのプリントを行う。

【0018】

図2は、本発明の実施の形態に係る無線通信デバイス装置の代表、すなわち、携帯もしくは可搬性の装置の代表としてのデジタルスチルカメラ2（以下、デバイス2）のブロック構成図である。

【0019】

同図において、201はデバイス全体の制御を司るCPUであり、202はCPU201のワークエリアとして使用されるRAMである。203はCPU201の処理手順を記憶しているROMである。ただし、ROMは書き換えが可能な不揮発性メモリ、例えばフラッシュメモリで構成される。204は画像処理部であり、撮像された画像をデジタル画像データに変換するのに用いられる。205は各種表示の制御部である。206は液晶表示器であり、撮像した画像の確認及び各種設定を行う際のメニューを表示するために使用される。207は発光ダイオードであり、デバイス2の処理状態を示すインジケータとして使用される。208は外部記憶装置の制御部であり、メモリソケット209に挿入されたコンパクトフラッシュ（登録商標）（R）やメモリースティック（R）等の記憶媒体へのデジタルデータの書き出し及び、記憶媒体に記憶されているデジタルデータの読み込みの制御を行う。210はUSBインターフェースの制御部であり、USBコネクタ211で他のUSBインターフェースを持つ装置と接続される。212は暗号処理部であり、認証情報や無線データ通信の暗号化を行うために使用される。213はリアルタイムクロックであり、認証期間カウントやアクセス時間記録を行うために使用される。222は無線通信を行うための無線通信部、223は無線通信を行うためのアンテナである。214は各種操作を行うボタン等の制御部であり、操作キー215、認証処理開始を指示する操作ボタン216、リセットボタン217の操作情報をCPU201へ伝えるために使用される。218はデバイス2の撮像素子の制御部であり、CCD219の制御を行う。220は光学ユニットの制御部であり、主としてレンズ及びその駆動系で構成される光学ユニット221の制御を行う。

【0020】

図3は、本実施形態に係る無線通信ホスト装置（実施形態ではプリンタ装置）1における無線通信部120のブロック構成図である。

【0021】

なお、デバイス装置（実施形態ではデジタルカメラ）2における無線通信部222も同様な構成であるものとし、デジタルカメラにおける無線通信部222の説明は省略する。また、実施形態では、説明を簡単なものとするため、IEEE802.11bのアドホックモードを前提にして説明するが、他の無線通信規格でも構わない。

#### 【0022】

図中、303は無線通信部の全体の制御を司る制御部であり、CPUや不揮発性メモリが内蔵されているものとする。304は通信プロトコルのリンク管理部、305は無線のベースバンド部であり、RF部306とアンテナ121で電波の送受信を行う。307はRFパワー制御部であり、電波の送受信パワーの制御を行う。308はRFパワー計測部であり、電波の送受信パワーの計測を行う。

#### 【0023】

以上、実施形態におけるホスト1及び、デバイス2の構成を説明した。

#### 【0024】

次に、上記構成に基づいて、ホスト1とデバイス2とを相互に認識し、無線通信接続に必要な通信パラメータ及びアドレス識別子等の認証情報を簡便に設定する方法を説明する。

#### 【0025】

図4は、それぞれ、無線通信ホスト装置であるプリンタ装置1（以下、ホスト1、総称してホストとする）と、無線通信デバイス装置であるデジタルスチルカメラ2、携帯電話3、PDA4（以下、デバイス2、デバイス3、デバイス4、総称してデバイスとする）との認証前の状態の一例を示した図である。

#### 【0026】

デバイス2、3、4には、図3に示した無線通信部120と無線通信に用いられるアンテナ121と同様の構成を備えるものとする。ホストとデバイスは、この無線通信部を用いて認証情報の交換、無線データ通信路の確立及び無線データ通信を行う。

#### 【0027】

ここで、ホスト1と、デバイス2との間で認証を行う場合の動作の一例を簡単に説明する。

#### 【0028】

まず、ホスト側の認証処理を開始するために、ホスト1のボタン116を押下すると、ホスト1は認証モードへ移行し、通常の無線データ通信（印刷データの受信処理）よりもRFパワーを低下させて、ホスト1の認証圏351を、例えば数十センチメートルに制限する。同様にデバイス側の認証処理を開始するために、デバイス2の操作キー215を操作してデバイス2を認証モードへ移行すると、デバイス2は無線データ通信中よりもRFパワーを低下させて、デバイス2の認証圏352を、例えば数十センチメートルに制限する。

#### 【0029】

図4に示すように、ホスト1と、デバイス2、デバイス3、及びデバイス4とは、互いの認証を行わない距離、すなわち認証時のホスト1の認証圏351外、及びデバイス2の認証圏352外に置かれているため、この状態でホスト1が認証可能なデバイスを探しても、デバイス2を発見する事ができず、認証は行われない。

#### 【0030】

次に、図5に示すように、ホスト1と、デバイス2を共に認証モードへ移行させた後、認証圏352をもつデバイス2をホスト1の認証圏351内に近づけると、ホスト1とデバイス2は、互いの無線通信部120及び222とアンテナ121及び223を用いて相互を検出、認識し、無線通信接続に必要な通信パラメータ及びアドレス識別子等の認証情報を交換する。なお、デバイス3と、デバイス4とは、認証モードに移行したとしても、ホスト1の認証圏351外であるため、相互の検出と認識及び認証情報の交換は行われない。

#### 【0031】

図6は、認証モードへ移行したホスト1とデバイス2の、認証処理中の動作と液晶表示器の表示の一例を示した図である。まずは、認証モードへ移行したホスト1の動作の説明をする。

#### 【0032】

認証モードへの移行指示を行うと、ホスト1は、無線データ通信中よりもRFパワーを低下させて、ホスト1の認証圏351を、通常の無線通信の通信圏と比較し、十分に狭い範囲（例えば数十センチメートルの範囲）に制限する。認証モードへ移行したホスト1はその液晶表示器106に無線接続対象とするデバイスをホスト1に接近させるように指示を表示する。このとき、液晶表示器106に表示する内容は文字列、アイコン及びホスト1に登録済みの実写画像等を用いると良い。なお、液晶表示器106での表示のほかに、発光ダイオード107の点灯及び点滅によるインジケータで、ホスト1が認証処理中であることを明示しても良い。

#### 【0033】

次に、認証モードへ移行したデバイス2の動作の説明をする。認証モードへの移行を指示すると、デバイス2は、無線データ通信中よりもRFパワーを低下させて、デバイス2の認証圏352を、ホスト1と同様に十分に狭い範囲（例えば数十センチメートル）に制限する。認証モードへ移行したデバイス2はその液晶表示器206に無線接続対象とするホストへデバイス2を接近させるように指示を表示する。このとき、液晶表示器206に表示する内容は文字列、アイコン及びデバイス2に登録済みの実写画像等を用いると良い。なお、液晶表示器206での表示のほかに、発光ダイオード207の点灯及び点滅によるインジケータで、デバイス2が認証処理中であることを明示しても良い。

#### 【0034】

本実施形態は、ホストとデバイスの装置間距離や指向性によるRFパワーの変位を利用して、本当に無線データ通信を行いたい相手装置（以下、真の接続対象とする）を検出、識別することを特徴とする。ここで、本実施形態として、ホストとデバイスとのRFパワーが、装置間距離や指向性でどのように変位するかを図7及び図8で説明する。

#### 【0035】

図7(a)、(b)は、認証処理中のホスト1と、真の接続対象とするデバイス2（以下、真のデバイス）のRFパワーと装置間距離特性を示す図である。認証モードに移行した真のデバイスをホストに接近させるように位置701から位置702に移動すると、図7(b)のグラフに示すようにホストの受信するRFパワー703は符号704から符号705へ変位する。このRFパワーの変位をホストのRFパワー計測部308で計測し、真のデバイスかどうかを判定する。逆に、認証モードに移行した真のデバイスをホストから遠ざけるように位置702から位置701に移動してもRFパワー703は変化するため、この変位をホストのRFパワー計測部308で計測し、真のデバイスかどうかを判定しても良い。また、ホスト及びデバイスのアンテナ構成により、図7(b)のグラフに示すように、ホストとデバイスを接近させると、ホストの受信するRFパワー706が符号707から符号708へ低下する場合においても、上記例のように、RFパワーの変位をホストのRFパワー計測部308で計測し、真のデバイスかどうかを判定できる。

#### 【0036】

図8(a)、(b)は、認証処理中のホストと、真のデバイスのRFパワー指向特性を示す図である。認証モードに移行した真のデバイスを、ホストの認証圏351内にある状態で回転すると、図8(b)のグラフに示すように、デバイスのアンテナの指向性により、ホストの受信するRFパワー801は符号802から符号803へ変位する。この変位をホストのRFパワー計測部308で計測し、真のデバイスかどうかを判定する。

#### 【0037】

RFパワーの変化とビットレート、ビットエラーレート及び転送効率の変化は相関関係にある場合が多いことから、上記RFパワーという記述を、ビットレート、ビットエラーレート及び転送効率等のデータ列を扱うものに置き換えて、変位の検出方法をホストのRFパワー計測部308でのRFパワー計測から、無線通信制御部303での数値計算に置

き換えても上記の変位検出方法は成立する。以下、RF パワー、ビットレート、ビットエラーレート及び転送効率等のデータ列を扱うものを総称して、RF パワーとする。

#### 【0038】

図9 (a) 乃至 (c) は、ホスト装置とデバイス装置が認証処理を開始し、ホストの認証圏351内に真のデバイスと他のデバイスがある場合に、真のデバイスを検出及び識別するための処理を説明するための図である。

#### 【0039】

真のデバイスと他のデバイスがともに認証モードであるとして、ある時間に真のデバイスを移動または回転させたとき、ホストが真のデバイスから受信するRF パワーが時間の二乗に比例するとした場合、時間  $t_1$  から  $t_2$  の間で、ホストが受信するRF パワーは、図9 (a) のグラフのように符号903から符号904に変化する。他のデバイスは移動または回転しないため、 $t_1$  から  $t_2$  の間でRF パワーは符号913から符号914と変化しない。

#### 【0040】

時間  $t_1$  と  $t_2$  の近傍において、ホストは真のデバイスと他のデバイスから受信するRF パワーを複数回サンプリングし、1次微分値をとると、図9 (b) のグラフのようにホストが受信する真のデバイスからのRF パワー1次微分値は符号905から符号906に変化する。対して他のデバイスからのRF パワーの1次微分値はゼロである。この1次微分値の変位を見ることにより、真のデバイスと他のデバイスの検出及び識別を行うことができる。ここで、1次微分値の変位の無かった他のデバイスは、真の接続対象ではないと識別されるため、ホストは認証情報の交換は行わない。

#### 【0041】

さらに、時間  $t_1$  と  $t_2$  の近傍において、ホストが真のデバイスと他のデバイスから受信するRF パワーを複数回サンプリングし、2次微分値をとると、図9 (c) に示すグラフのように、ホストが受信する真のデバイスからのRF パワー2次微分値は符号907から符号908で一定である。対して他のデバイスからのRF パワーの2次微分値はゼロである。この2次微分値の変位を見ることにより、真のデバイスと他のデバイスの検出及び識別を行っても良い。

#### 【0042】

なお、図9 (a) 乃至 (c) に示してあるホストが受信するデバイスからのRF パワーの時間変化は一例であり、実際はホストが真のデバイスから受信するRF パワーが時間の二乗に比例するとも限らず、ホストが他のデバイスから受信するRF パワーが一定であるとも限らない。そこで、ホストでは真のデバイスの検出及び識別精度を上げるため、想定する無線通信システムに合ったサンプリング時間とサンプリング回数、及び微分回数とを選択すると良い。

#### 【0043】

以下、前述した真のデバイスを検出及び識別するための処理を用いて、ホストが真のデバイスとの認証処理を行う手順を説明する。

#### 【0044】

図10A、10Bは、ホストが認証処理を開始してから認証処理を終了するまでの処理手順を示すフローチャートである。この処理手順に係るプログラムは、ROM103に格納されているものである。

まず、ホストに配設されているボタン等を操作して、ホストを認証モードに移行させると、ホストは送受信RF パワーをデータ通信を行うモードよりも低下させて無線信号到達距離を狭め、認証圏を設定する(ステップS101)。

#### 【0045】

次に図11に示すようなインクワイアリ(Inquiry: 問合せ、接続要求と同義)信号1101を生成し記憶する(ステップS102)。インクワイアリ信号1101には任意のデータ列1102と、インクワイアリ応答の繰り返し時間間隔を指定するデータ列1103を内包している。任意のデータ列1102は、インクワイアリ信号を受信したデ

バイスが、この任意のデータ列 1102 (照合データでもある) をインクワイアリ応答に内包して返信するものであり、ホストが応答であるか、更には、データ列のビットレート、ビットエラーレート及び転送効率等の変位を検出するために用いられる。インクワイアリ応答の繰り返し時間間隔を指定するデータ列 1103 (時間間隔を指示する情報) は、デバイスから返信されるインクワイアリ応答の繰り返し時間間隔を判定するために用いられる。

#### 【0046】

ホストはインクワイアリ信号 1101 を生成すると、デバイス探索のために認証圏内にインクワイアリ信号 1101 を送信する (ステップ S103)。

#### 【0047】

このとき、ESSID (Extended Service Set Identifier) は仮の文字列、WEP キー (Wired Equivalent Key) 無し、チャンネルは "1" に設定して送信する。ただし、認証処理が成功した場合には、認証情報として、真の ESSID、WEP キー、チャンネルを送信し、それ以降はこれを用いて通信を行うものとする。

#### 【0048】

ホストの認証圏内に認証モードに移行しているデバイスが存在すると、デバイスから図 12 に示すようなインクワイアリ応答 1201 が返信されるため、ホストはインクワイアリ応答を受信したかどうかを判定する (ステップ S104)。デバイスが返信するインクワイアリ応答 1201 には、ホストからのインクワイアリ信号 1101 で指定されたデータ列 1102 を含むデータ列 1202 と、デバイスの ROM に保存されている MAC アドレス等の固有コード 1203 を内包している。固有コード 1203 はホスト側での MAC アドレスフィルタリング等の無線接続制御に用いられるほか、ホスト認証情報の生成に用いられる。

#### 【0049】

もし、所定の許容時間範囲内で、インクワイアリ応答 1201 が返信されない場合、ホストの認証圏内に認証モードに移行しているデバイスが存在しないと判断し、ホストは認証モードを終了し、ステップ S118 に進み、通常のデータ通信状態にするため RF パワーを復帰する。

#### 【0050】

ホストは 1 回目のインクワイアリ応答 1201 を受信すると、その受信 RF パワーを複数回計測・記憶し (ステップ S105)、インクワイアリ応答 1201 のデータ列の一部を記憶する (ステップ S106)。

#### 【0051】

インクワイアリ応答 1201 は、インクワイアリ信号 1101 に内包されたデータ列 1103 で指定された時間間隔でホストへ返信されることから、ホストは再びインクワイアリ応答 1201 を受信したかどうかを判定する (ステップ S107)。ホストは 2 回目のインクワイアリ応答 1201 を受信すると、その 2 回目の受信 RF パワーを複数回計測・記憶し (ステップ S108)、2 回目のインクワイアリ応答 1201 のデータ列の一部を記憶する (ステップ S109)。

#### 【0052】

ホストは、1 回目と 2 回目のインクワイアリ応答 1201 の受信 RF パワー及びデータ列を記憶すると、インクワイアリ応答 1201 の繰り返し時間が、データ列 1103 で指定した時間と同一かどうかを判定する (ステップ S110)。ここで、インクワイアリ応答 1201 の繰り返し時間が異なっていた場合は、ホストは真のデバイスからの応答ではないと判定し、認証モードを終了する。

#### 【0053】

次にホストは、インクワイアリ応答 1201 に任意のデータ列 1102 が内包されているかを判定する (ステップ S111)。インクワイアリ応答 1201 にホストが指定した任意のデータ列 1102 が内包されていない、または異なるデータ列が内包されていた場

合は、ホストは真のデバイスからの応答ではないと判定し、認証モードを終了する。

【0054】

次にホストは、1回目と2回目のインクファイアリ応答1201の受信RFパワーの変位を計算する(ステップS112)。ステップS112での計算は図9を用いて説明したような処理を用いると良い。ステップS112で計算された結果を元に、ホストは受信したインクファイアリ応答1201のRFパワーの変位が、システムの規定する所定範囲内に収まっているかどうかを判定する(ステップS113)。

【0055】

ここで、RFパワーの変位が無い、または変位がシステムの規定する範囲外であった場合は、ホストは認証モードを終了する。

【0056】

なお、ここで言う変位は、その正負の符号は無視するため、差分の絶対値を取る。そして、その変位が実質的に0(正確には0に近い閾値T1以下)か、閾値T2( $T2 > T1 > 0$ )以上の場合には、認証失敗として判定し、ホストは認証モードを終了する。

【0057】

また、RFパワーの変位がシステムの規定する範囲内(閾値T1より大きく、T2未満)であった場合は、RFパワーが変位したデバイスが唯一かどうかを、インクファイアリ応答のデータのデバイス固有コードが一致するかどうかに基づいて判定する(ステップS114)。認証圏内にRFパワーが変位したデバイスが複数あった場合は、ホストは認証モードを終了する。RFパワーが変位したデバイスが唯一であった場合は、ホストはそのデバイスを真のデバイスと認識し、真のデバイスの認証情報を生成し記憶する(ステップS115)。

【0058】

次に、生成した認証情報を真のデバイスへ送信する(ステップS116)。その後、真のデバイスへ認証終了を通知し(ステップS117)、認証モードを終了してRFパワーを復帰する(ステップS118)。認証処理終了後、すぐに無線データ通信を行わない場合は、認証モード終了後RFパワーをOFFにして、ホストをアイドル状態にしても良い。

【0059】

以上のフローが終了すると、ホストとデバイスは交換した認証情報を用いて無線通信路353を確保し、無線データ通信を行うことができるようになる。実施形態の場合、ホストはプリンタ、デバイスはデジタルカメラであるので、デジタルカメラで撮像された画像のプリント出力処理が行われることになる。

【0060】

以上、図10A、10Bを用いて述べたホストの認証フローにおいて、真のデバイスの判定条件は、以下のプロセス(S151)～(S156)に示すように分けることができる。

- ・ステップS151：ステップS101からステップS104において、ホスト認証圏内か認証圏外かの判定、
- ・ステップS152：RFパワー、ビットレート、ビットエラーレート、及び転送効率の計測、
- ・ステップS153：インクファイアリ応答の繰り返し時間が、ホストの指定した繰り返し時間と同一かの判定、
- ・ステップS154：インクファイアリ応答にホストが指定した任意のデータ列が含まれているかを判定、及び、
- ・ステップS155：RFパワー、ビットレート、ビットエラーレート、及び転送効率の変位があるかを判定、
- ・ステップS156：RFパワー、ビットレート、ビットエラーレート、及び転送効率に変位したデバイスが唯一かどうかを判定する。

【0061】



なお、プロセス(S151)で判定する認証圏内、認証圏外の設定距離はいくらでも構わないが、認証圏が広すぎるとセキュリティの強度が低下し、さらに真のデバイス判定が困難になることから、できるだけ短距離であることが望ましい。つまり、実施形態で示しているように数十センチメートル程度が妥当であろう。

#### 【0062】

また、プロセス(S152)と同様のプロセスは図10A、10Bの例では2回繰り返しているが、複数回繰り返してデバイスの検出精度を上げて良い。

#### 【0063】

上記プロセス(S153)から(S155・S156)は順序は問わず、また、上記ステップに限らず他の判定ステップを組み合わせた、判定ステップを減らしても構わない。特に、ステップS151乃至S155の判定の少なくとも1つと、ステップS156との組み合わせで、デバイスが特定できる場合には、それを真のデバイスと判定しても構わない。

#### 【0064】

次に、デバイス側のホストとの認証処理を行う手順を説明する。図13は、デバイス(実施形態ではデジタルカメラ)が認証処理を開始してから認証処理を終了するまでのフローチャートである。このフローチャートに対応するプログラムは、ROM203に格納されるものでもある。

#### 【0065】

まず、デバイスに配設されているボタン等を操作して、デバイスを認証モードに移行させると、デバイスは送受信RFパワーをデータ通信を行うモードよりも低下させて無線信号到達距離を狭め、認証圏を設定する(ステップS201)。このとき、無線のパラメータは、ホスト側の認証処理開始時と同様にする。

#### 【0066】

ここで、デバイスの認証圏内に認証モードに移行しているホストが存在すると、ホストは図11に示すようなインクワイアリ信号1101を送信してデバイスを探索しているため、デバイスはインクワイアリ信号を受信したかどうかを判定する(ステップS202)。

#### 【0067】

もし、認証圏内に認証モードに移行しているホストが存在しない場合はインクワイアリ信号は受信されない。この場合には、ステップS210に進んで、デバイスは認証モードし、通常のデータ通信状態にするためRFパワーを復帰する。

#### 【0068】

また、デバイスがインクワイアリ信号を受信すると、図12に示すような1回目のインクワイアリ応答1201を生成し記憶する(ステップS203)。このインクワイアリ応答1201には、ホストから指定された任意のデータ列1102を含むデータ列1202と、デバイスのROMに保存されているMACアドレス等の固有コード1203を内包している。

#### 【0069】

次に、デバイスは1回目のインクワイアリ応答1201をホストに対して複数回送信する(ステップS204)。1回目のインクワイアリ応答送信後、デバイスは2回目のインクワイアリ応答1201を生成、記憶し(ステップS205)、2回目のインクワイアリ応答1201をホストに対して複数回送信する(ステップS206)。なお、1回目と2回目のインクワイアリ応答は、インクワイアリ応答の繰り返し時間を指定するデータ列1103で指定された繰り返し時間間隔でホストに送信する。先に説明したように、ホストが真のデバイスかそうでないかを判定するパラメータの一つとなるためである。

#### 【0070】

プロセス(S251)と同様のプロセスは図13の例では2回繰り返しているが、システムの構成により複数回繰り返しても良い。また、インクワイアリ応答1201の生成と記憶を1回だけ行うようにしても良い。

#### 【0071】

インクワイアリ応答1201を送信したデバイスは、ホストからの認証情報を受信したかを判定し（ステップS207）、ホストから認証情報が送信されない、またはホストからの認証情報を受信できない場合は認証モードを終了する。ホストから認証情報を受信したならば、デバイスはその認証情報を記憶する（ステップS208）。その後、ホストへ認証終了を通知し（ステップS209）、認証モードを終了してRFパワーを復帰する（ステップS210）。

#### 【0072】

以上のフローが終了すると、ホストとデバイスは交換した認証情報を用いて無線通信路353を確保し、無線データ通信を行うことができるようになる。

#### 【0073】

図14A、14Bは、図10A、10Bで述べたホストの認証プロセスフローと、図13で述べたデバイスの認証プロセスフローを合わせて示した認証処理フローである。処理内容は、既に説明した通りであるので、省略するが、特に図14Aのプロセス（S301）を繰り返し行うことで、真のデバイスの検出を容易にし、かつ、他の第三者のデバイスが認証情報を傍受するのを防ぐことができる。

#### 【0074】

なお、ホストとデバイスの双方に表示部を備え、認証処理が正常に完了した場合には、それぞれの表示部に、認証成功を示す表示（メッセージやLED点灯等）を行うようにすることが望ましい。万が一、一方のみに認証成功の表示が行われた場合には、意図しないデバイスやホストと認証処理をしてしまったことがわかるので、再度上記の処理を行えば良い。

#### 【0075】

以上説明したように本実施形態によれば、2つの無線通信装置が互いに認証を行う際には、それぞれのRFパワー下げる、すなわち、通信可能範囲を例えば数十センチメートル程度の距離でないと送受信できない状態することで、単一の無線通信手段を利用しながらも、他のデバイスや他のホストが圏内に入り込むことを除外することが可能となる。そして、ホストは、自身が設定したデータ列を含むインクワイアリ応答が、自身が設定した所定時間間隔で受信でき、尚且つ、そのインクワイアリ応答の受信強度に変化がある場合に限って、該当するインクワイアリ応答を発信したデバイスが認証対象デバイスとして判定する。従って、ホストの近くに意図しない他のデバイスが存在する場合であっても、目的とするデバイスをその範囲内にて移動、回転等を行えば、他のデバイスと容易に区別され、認証処理が完了することになる。

#### 【0076】

換言すれば、本実施形態にしたがえば、無線通信装置相互の接続対象の検出及び認証からデータ通信に至るまでを、単一の無線通信手段のみを用いて行うことができるため、無線通信装置の簡素化、省電力化及び小型化に有効である。また、無線通信装置相互の接続対象の検出及び認証時にはRFパワーをデータ通信を行う状態よりも低下させて、無線信号到達距離を狭めることから、認証情報の傍受の危険性が少なく高セキュリティである。さらに、第1の無線通信装置が真の接続対象とする第2の無線通信装置を検出する際には、RFパワー、ビットレート、ビットエラーレート及び転送効率等の変位を利用することから、第1及び第2の無線通信装置の認証圏内に、真の接続対象ではない無線通信装置が存在する状況においても、意図しない無線通信装置間での認証情報の交換を避けることができる。第1及び第2の無線通信装置間の認証情報の交換は、真の接続対象とする無線通信装置を相互に検出した後、自動で継ぎ目が行われることから、表示部や操作部の無い無線通信装置にも適用可能であり、使用者が認証情報を手動で設定したり、難しい操作をしたりすることを必要とせずに無線通信装置の認証を行うことができ、高セキュリティな無線通信システムとサービスを簡便に提供することができる。

#### 【0077】

なお、実施形態では、ホストとしてプリンタ装置、デバイスとしてデジタルカメラにつ

いて説明したが、これらの装置によって本願発明が限定されるものではない。要は、お互いに、RF パワー制御、並びに受信パワーの計測を行え、ホスト、デバイスそれぞれが相手と通信するための単一の通信手段を備えれば良い（図4に示されるデバイス3、4（形態電話やPDA）は通信手段を2つ備えているが、ホストと通信する手段は1つのみである点に注意されたい）。

#### 【0078】

従って、例えばホストはデスクトップパーソナルコンピュータ等の情報処理装置（ホスト）であり、もう一方もPDAやノートタイプのパーソナルコンピュータでも構わないであろう。

#### 【0079】

なお、実施形態では、デバイス装置とホスト装置の少なくとも一方が移動可能であることを前提として説明したが、ホスト装置とデバイス装置は、お互いに、RF パワー制御、並びに受信パワーの計測を行えれば良い。従って、ホスト装置及びデバイス装置に、実施形態の図7、図8で説明したRF パワー制御と同様の効果のあるRF パワー変調処理を行う回路またはソフトウェアが搭載されている場合、一方が移動しなくとも、お互いの認証圏内であれば、装置に配設されたボタンやキーを操作することによってRF パワー変調処理を行い、実施形態に沿った方法で認証処理を行うことができる。

#### 【0080】

パーソナルコンピュータ等の汎用情報処理装置はホストもしくはデバイスとして機能する場合には、当然、図10A、10Bまたは図13に示す処理を行うプログラムがインストールされることになるわけであるから、当然、本発明はそのようなコンピュータプログラムをも含むことになる。さらにまた、通常、コンピュータプログラムはCD-ROM等のコンピュータ可読記憶媒体に格納されていて、それをコンピュータにセットして、システムにコピーもしくはインストールすることで実行可能になるわけであるから、そのようなコンピュータ可読記憶媒体も本願発明の範疇になることも明らかである。

#### 【図面の簡単な説明】

#### 【0081】

【図1】実施形態における無線通信ホスト装置となるプリンタ装置のブロック構成図である。

【図2】実施形態における無線通信デバイス装置となるデジタルカメラのブロック構成図である。

【図3】実施形態における無線通信ホスト装置内の無線通信部のブロック構成図である。

【図4】実施形態におけるホスト装置と無線通信デバイス装置の認証前の状態の一例を示す図である。

【図5】実施形態における無線通信ホスト装置と無線通信デバイス装置の認証処理中の状態を示す図である。

【図6】実施形態における認証処理中の無線通信ホスト装置と無線通信デバイス装置それぞれの表示部の状態の一例を示す図である。

【図7】実施形態における無線通信ホスト装置と認証対象の無線通信デバイス装置の認証処理中のRFパワーの距離特性の一例を示した図である。

【図8】実施形態における無線通信ホスト装置と認証対象の無線通信デバイス装置の認証処理中のRFパワーの放射特性の一例を示す図である。

【図9】実施形態におけるホストが認証対象の無線通信デバイス装置を識別する際に用いる無線信号の特性を示す図である。

【図10A】実施形態における無線通信ホスト装置における認証処理手順を示すフローチャートである。

【図10B】実施形態における無線通信ホスト装置における認証処理手順を示すフローチャートである。

【図11】実施形態における無線通信ホスト装置が発信するインクワイアリ信号のデ

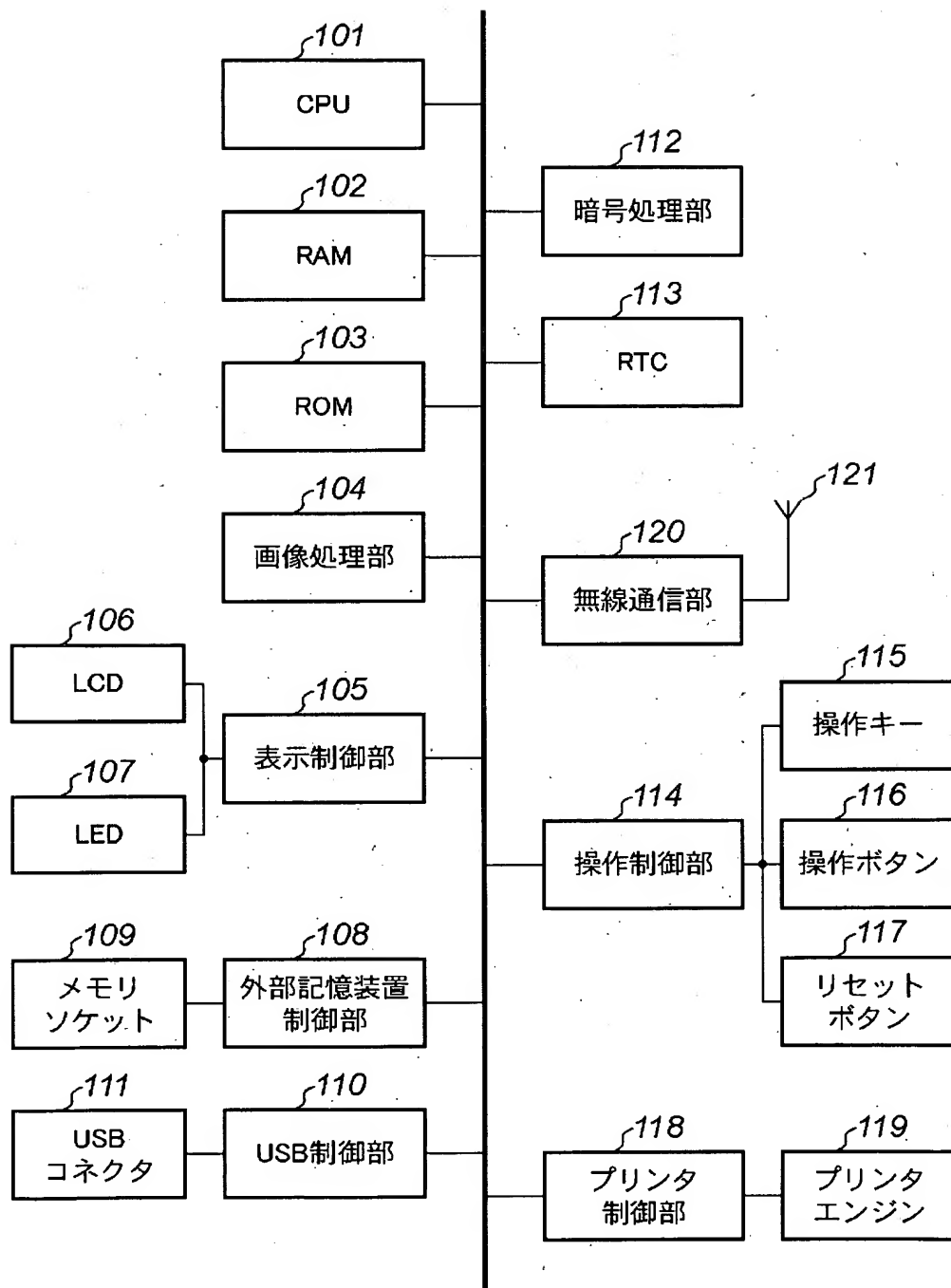
ータフォーマットを示す図である。

【図 1 2】実施形態における無線通信デバイス装置が応答するインクワイアリ応答信号のデータフォーマットを示す図である。

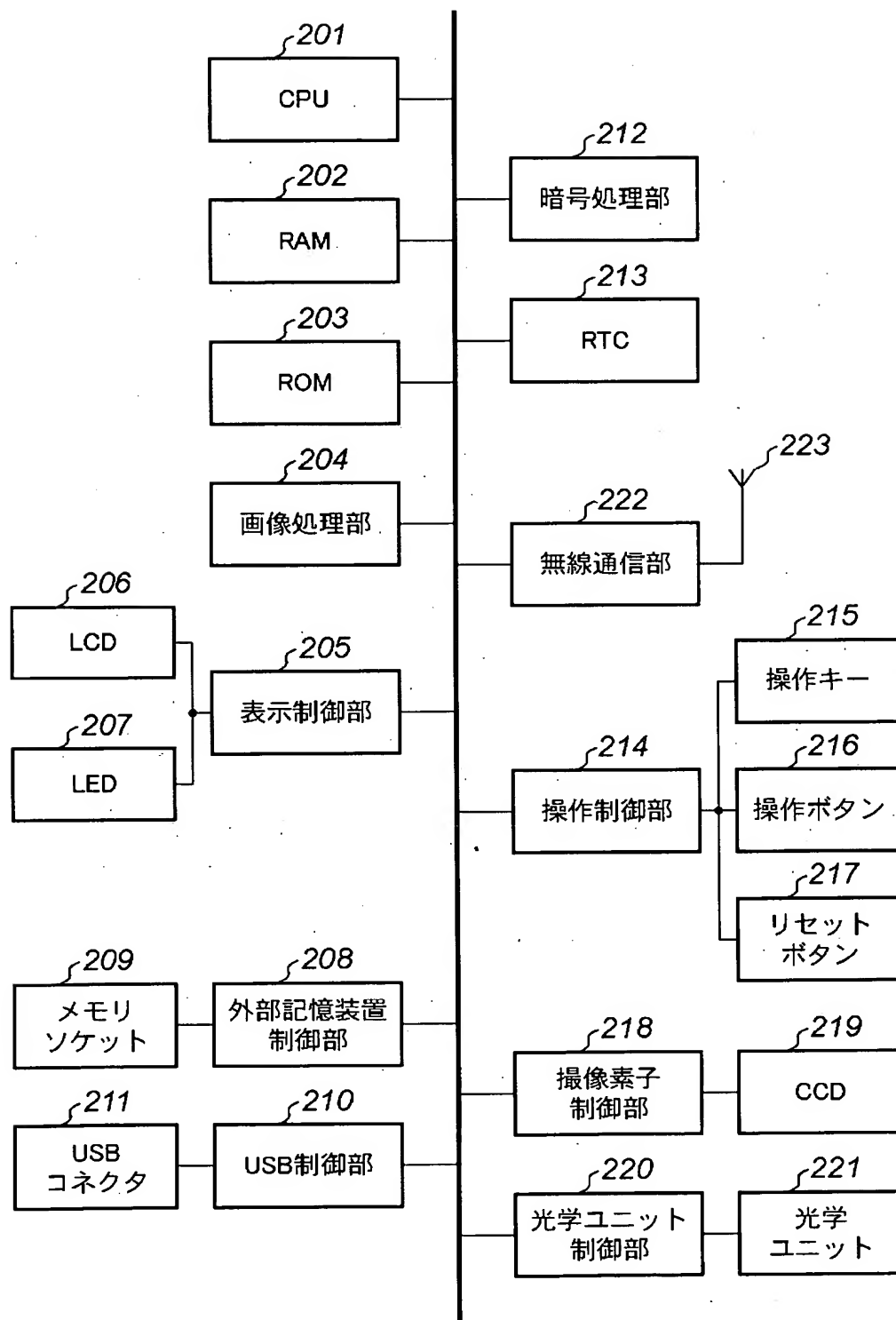
【図 1 3】実施形態における無線通信デバイス装置における認証処理手順を示すフローチャートである。

【図 1 4 A】実施形態における無線通信ホスト装置と無線通信デバイス装置の処理の関係を並列して示すフローチャートである。

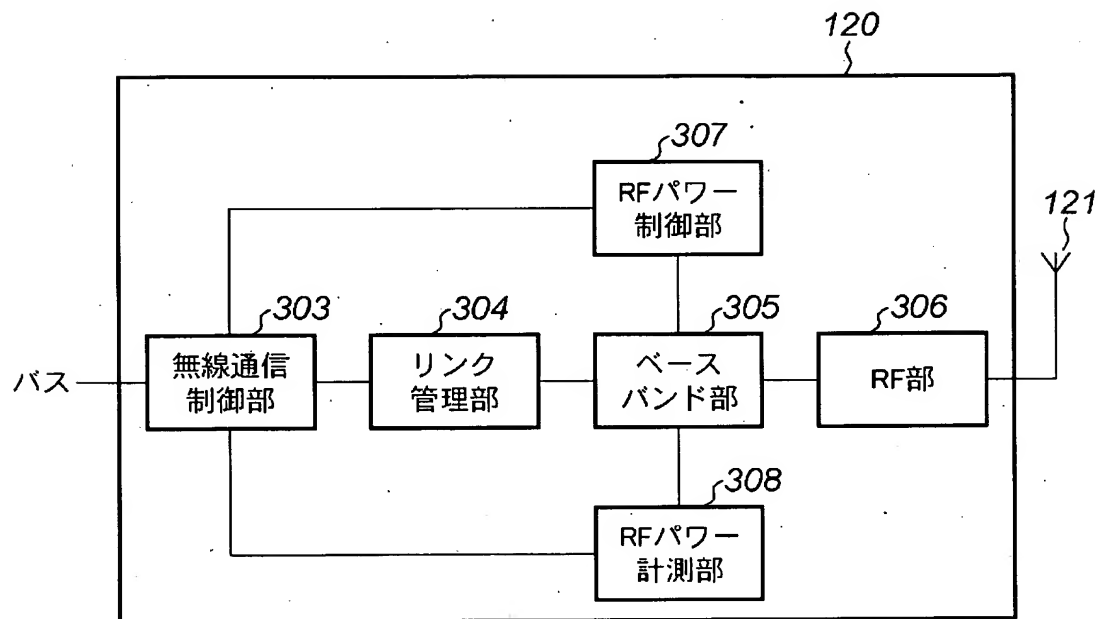
【図 1 4 B】実施形態における無線通信ホスト装置と無線通信デバイス装置の処理の関係を並列して示すフローチャートである。



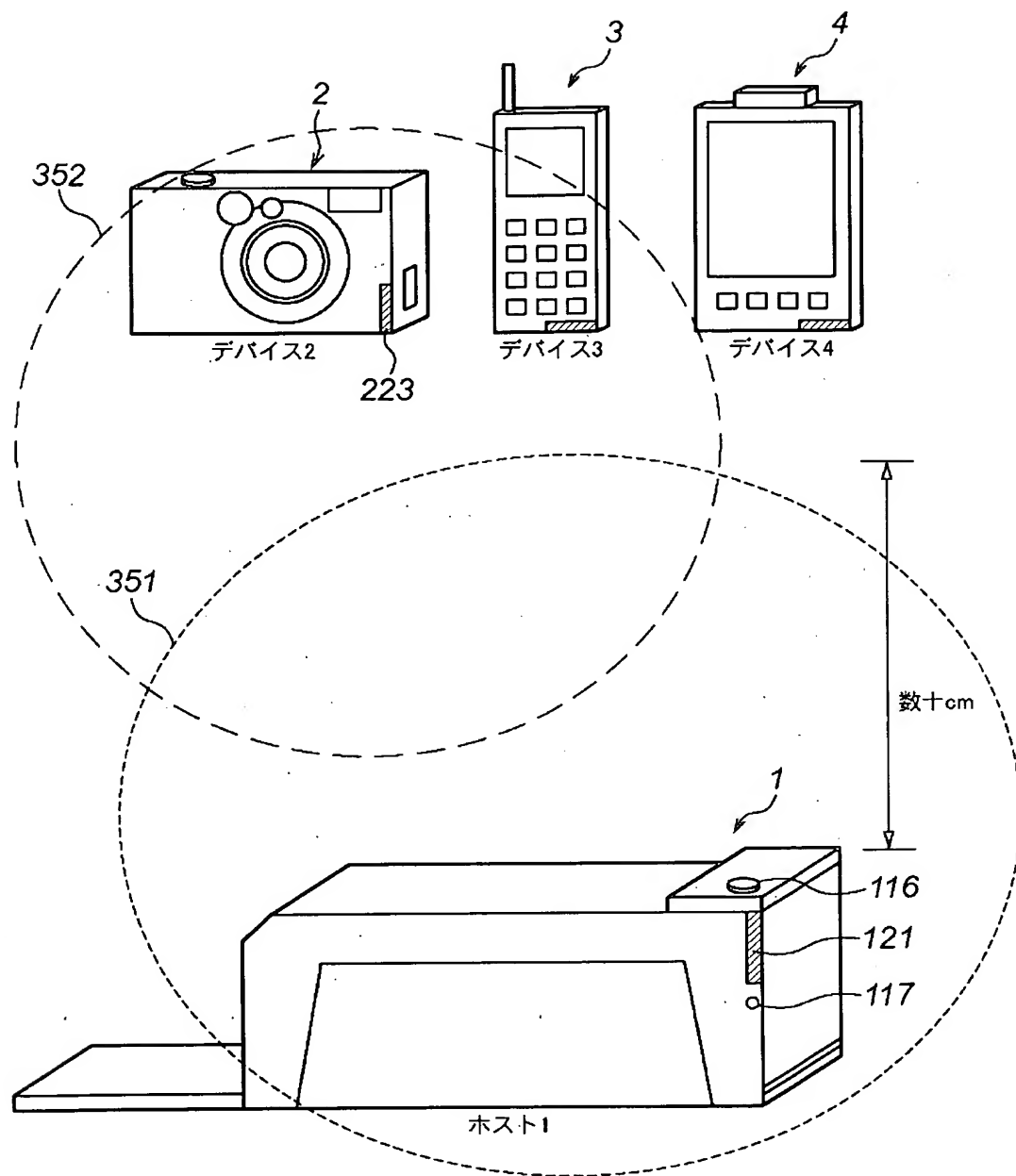
【図 2】



【図 3】

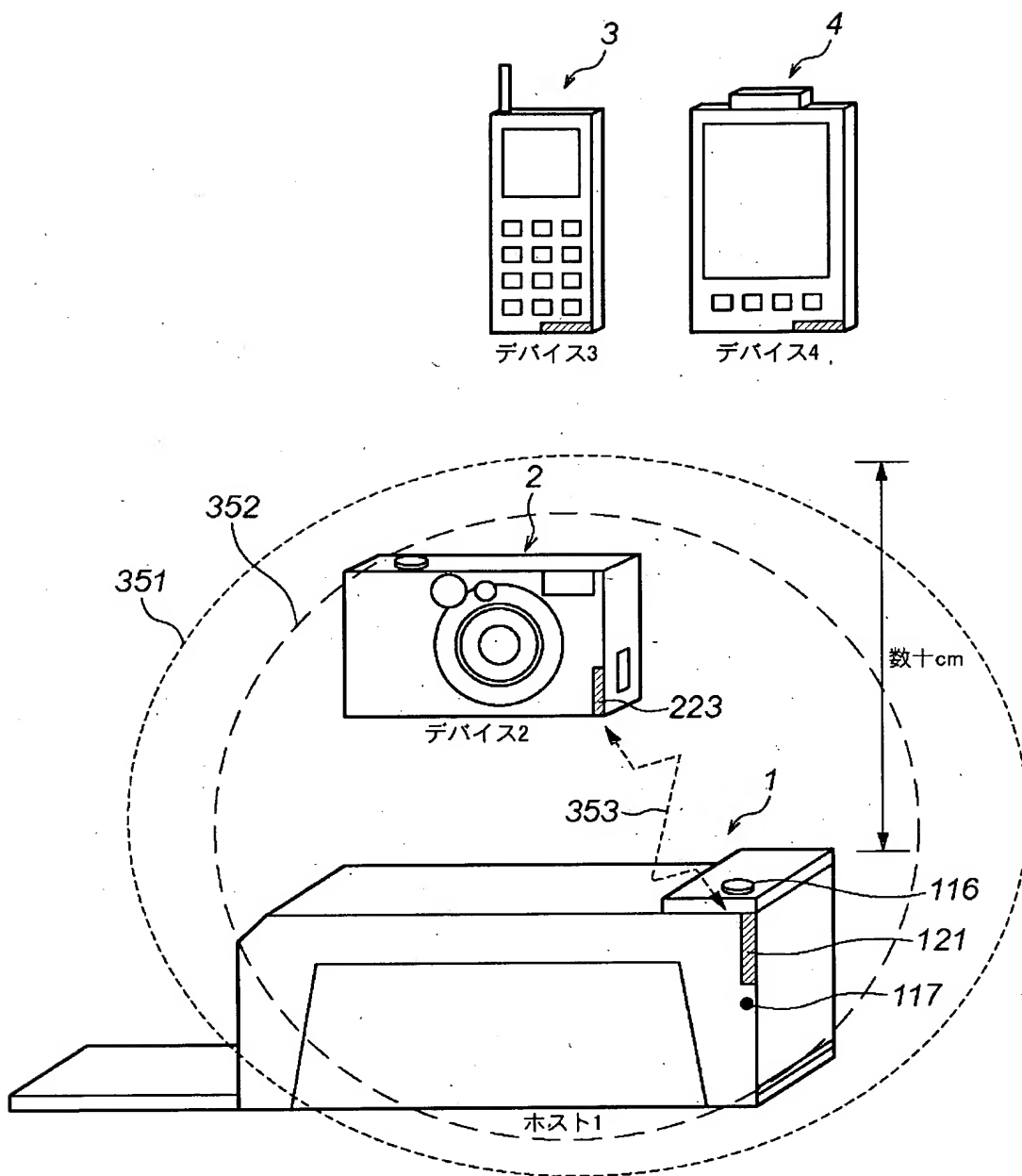


【図4】

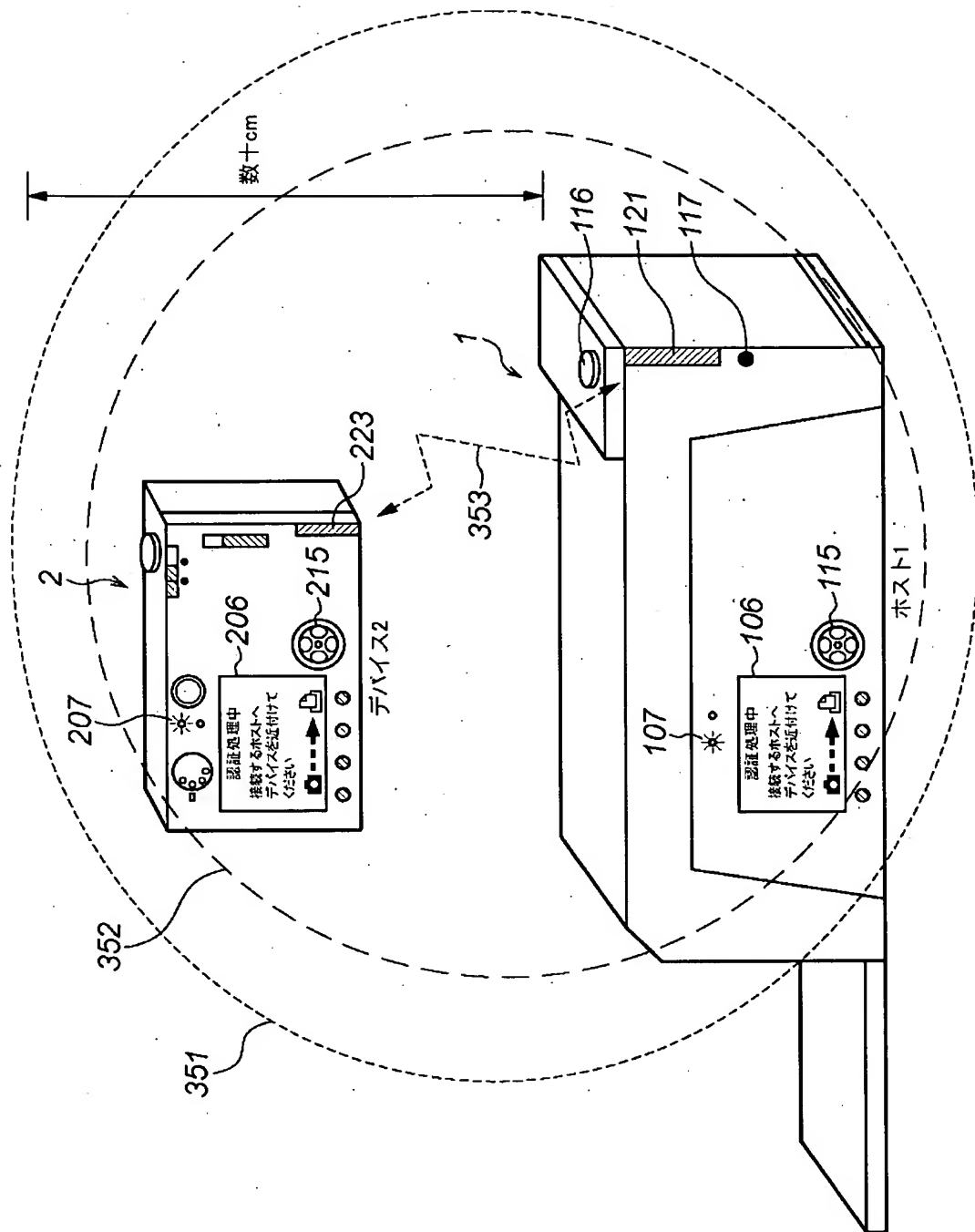




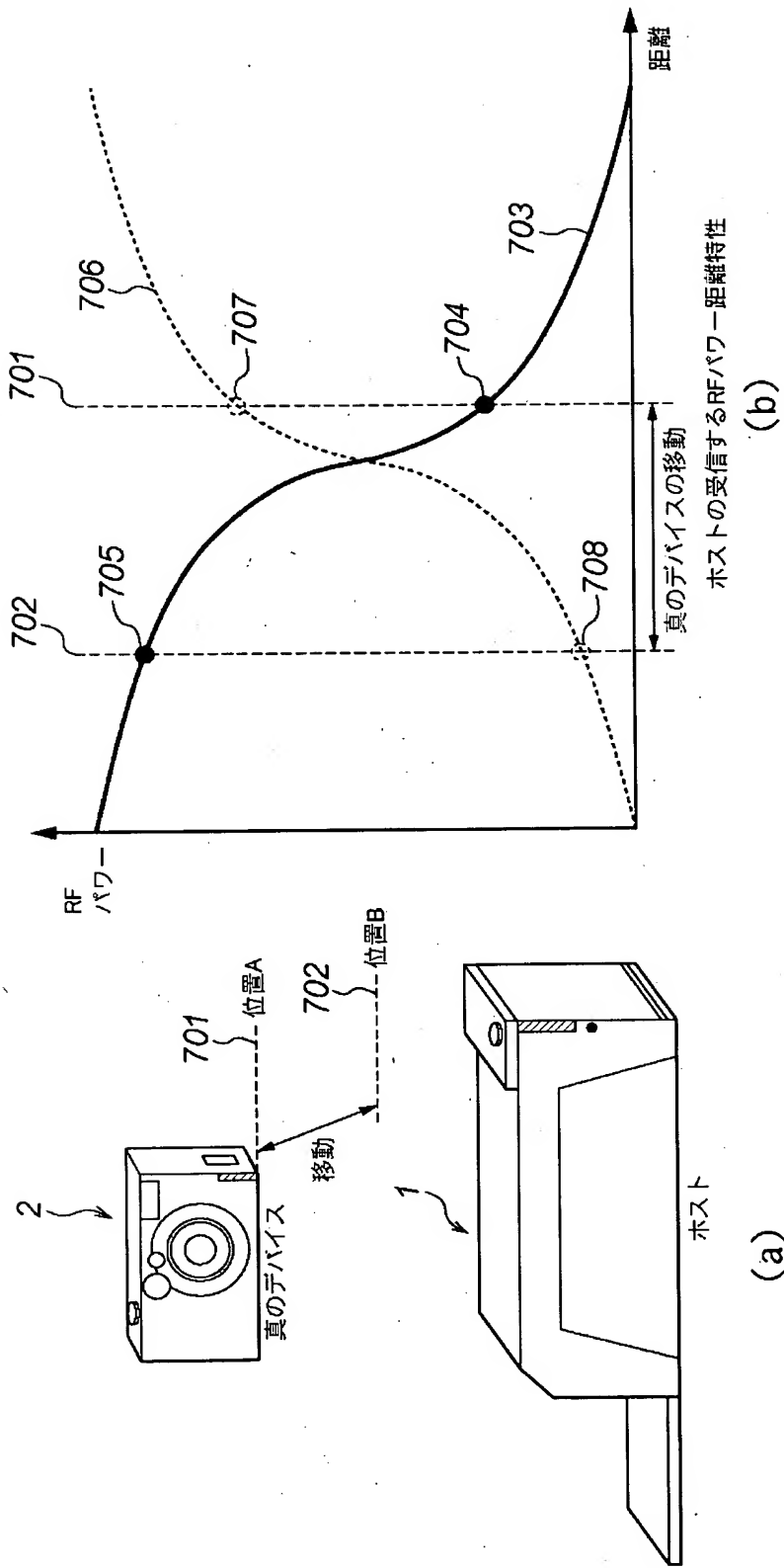
【図5】

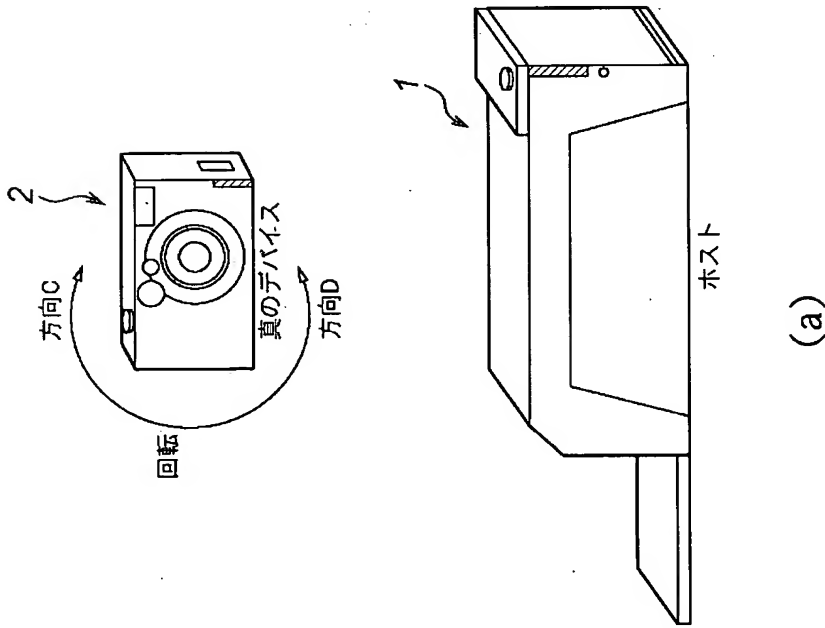
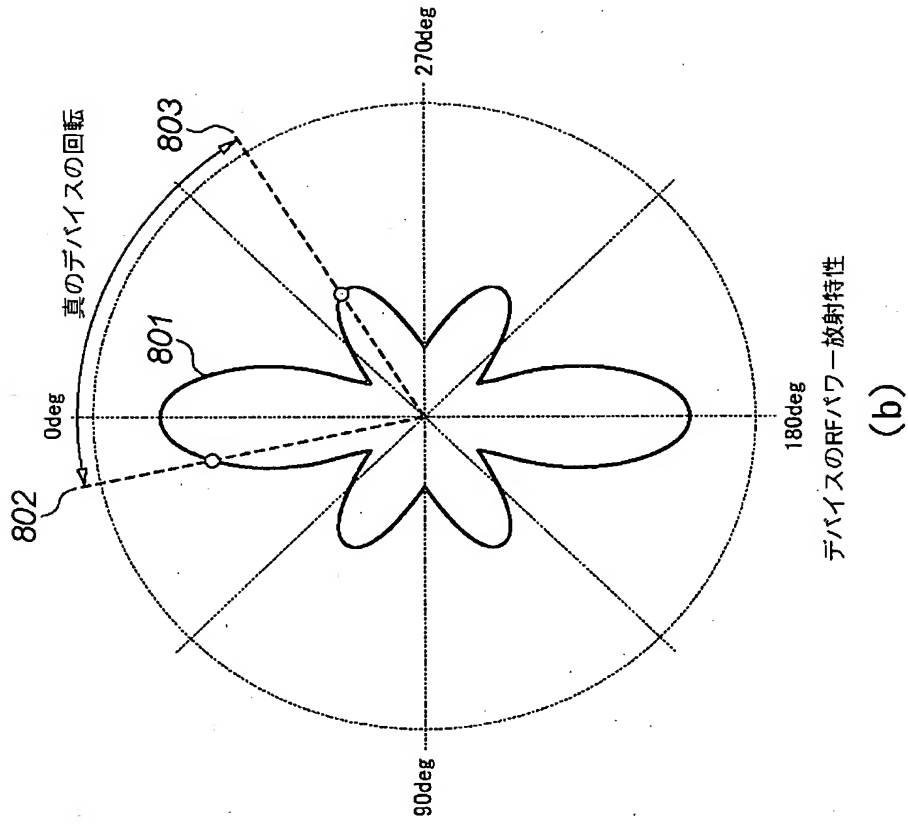


【図 6】

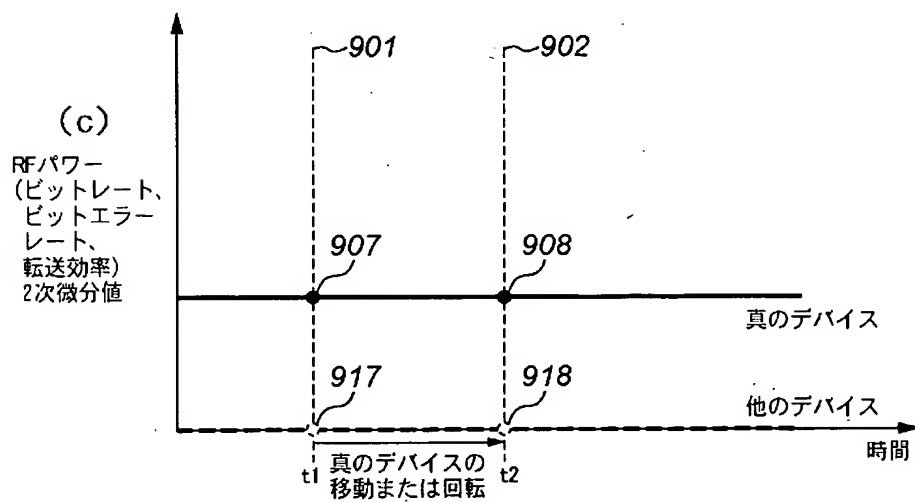
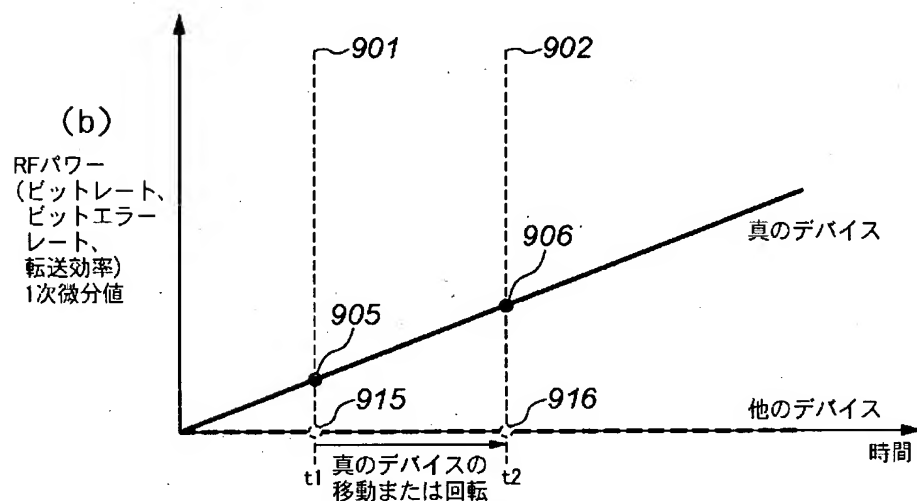
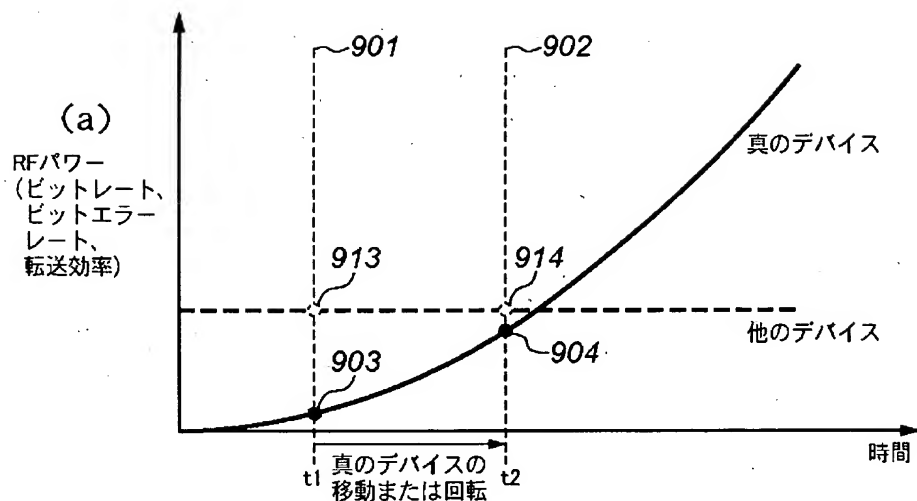


【図 7】

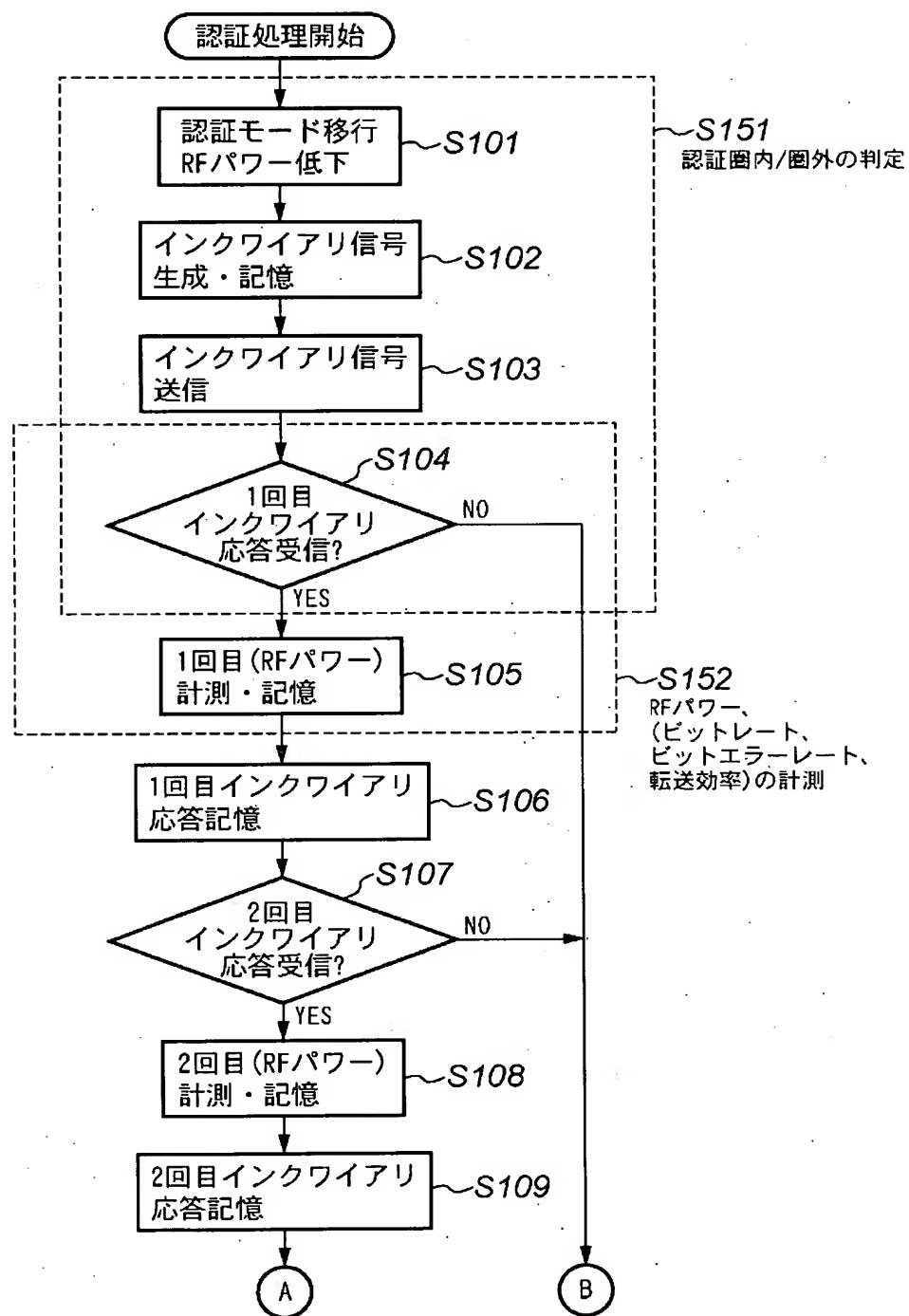




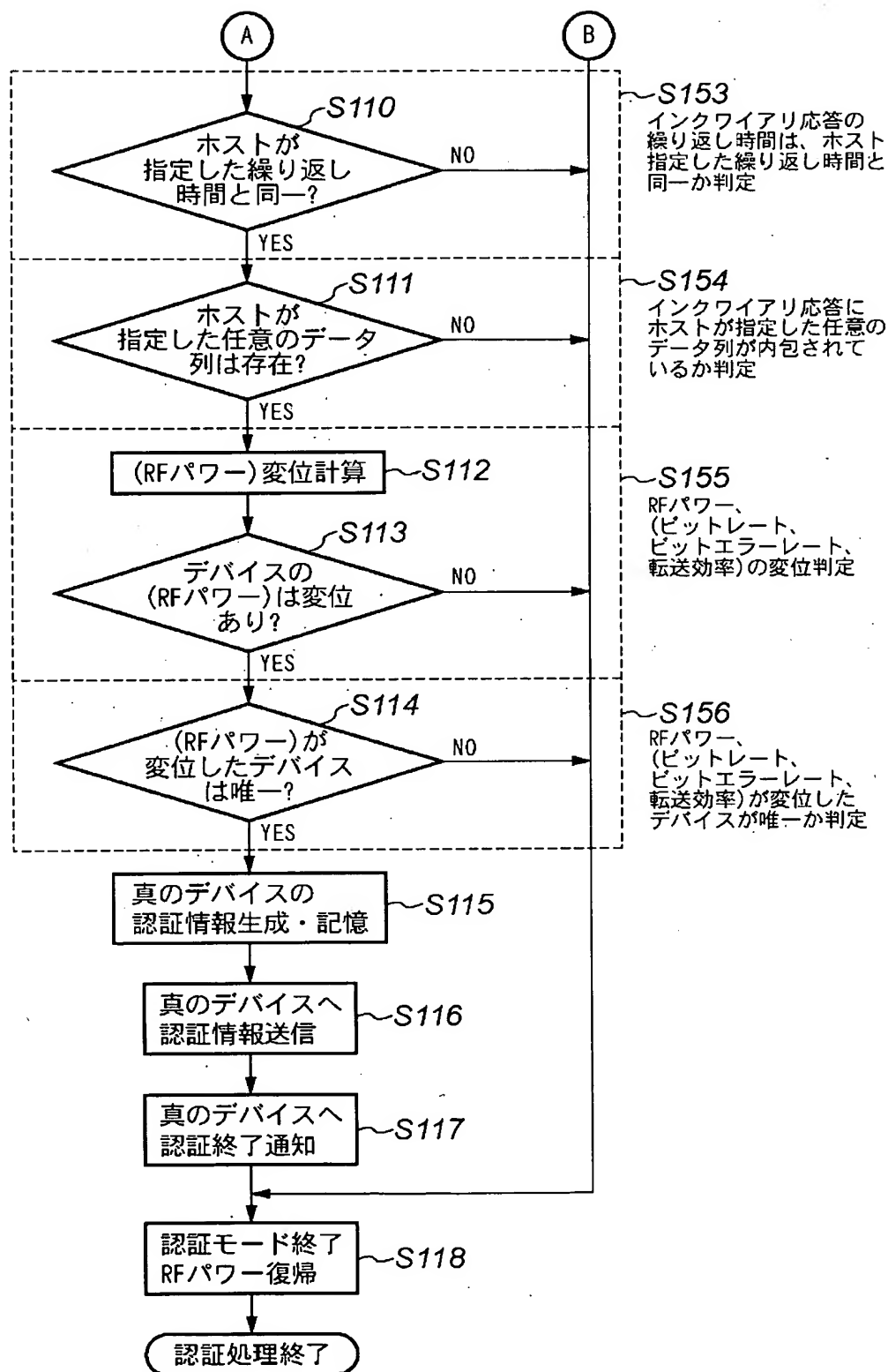
【図 9】



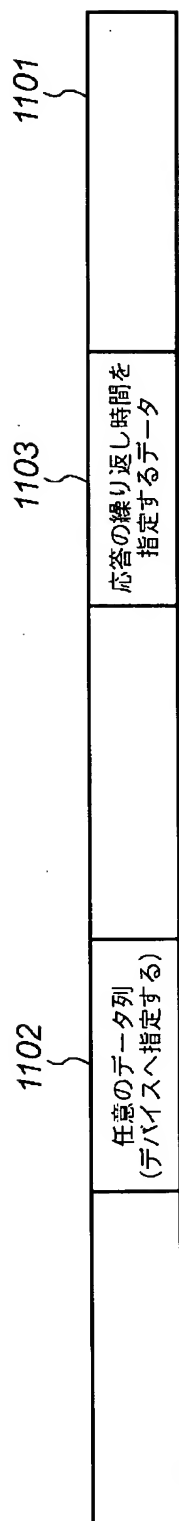
【図10A】



【図10B】

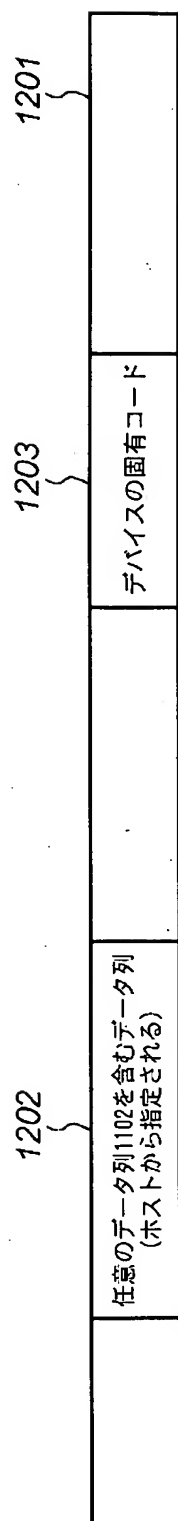


【図 1 1】

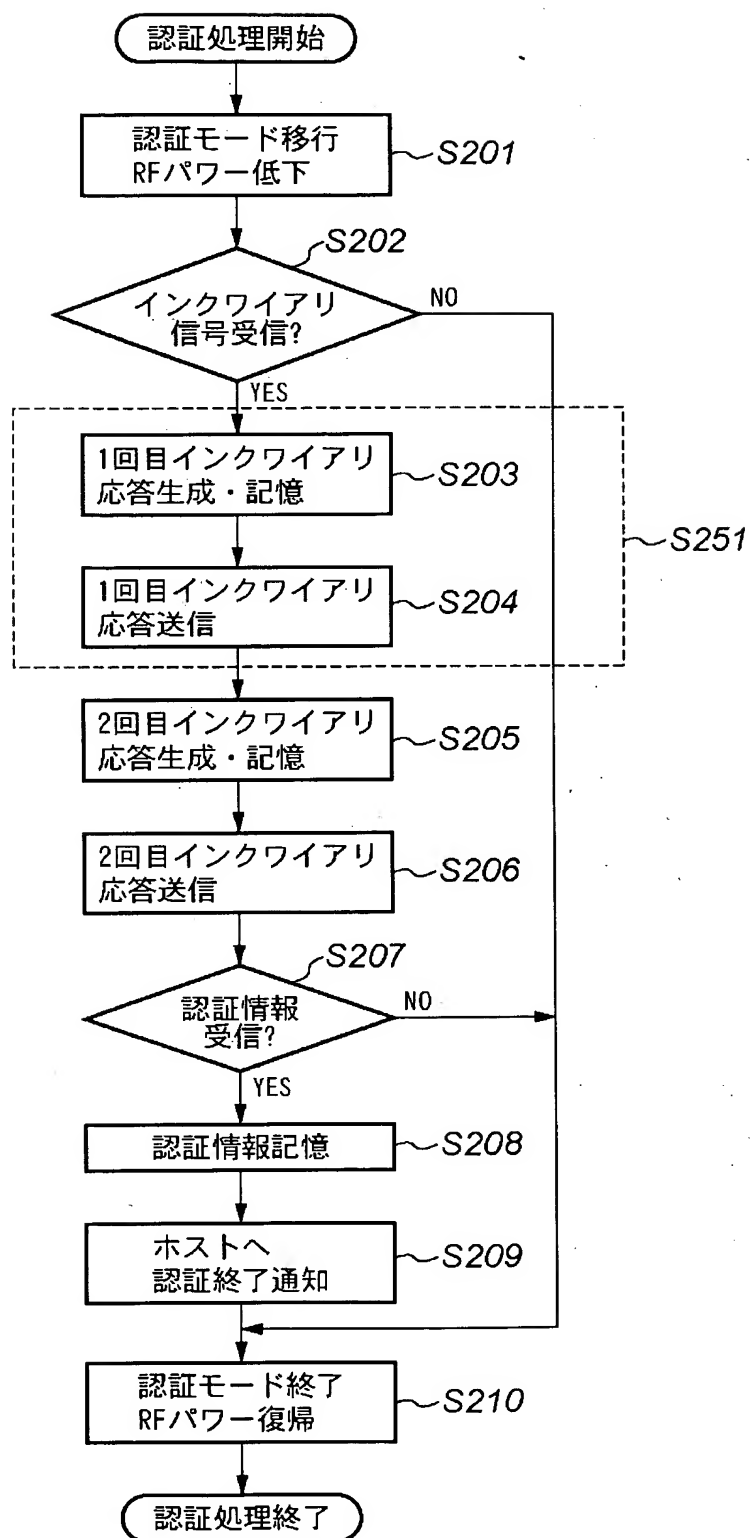




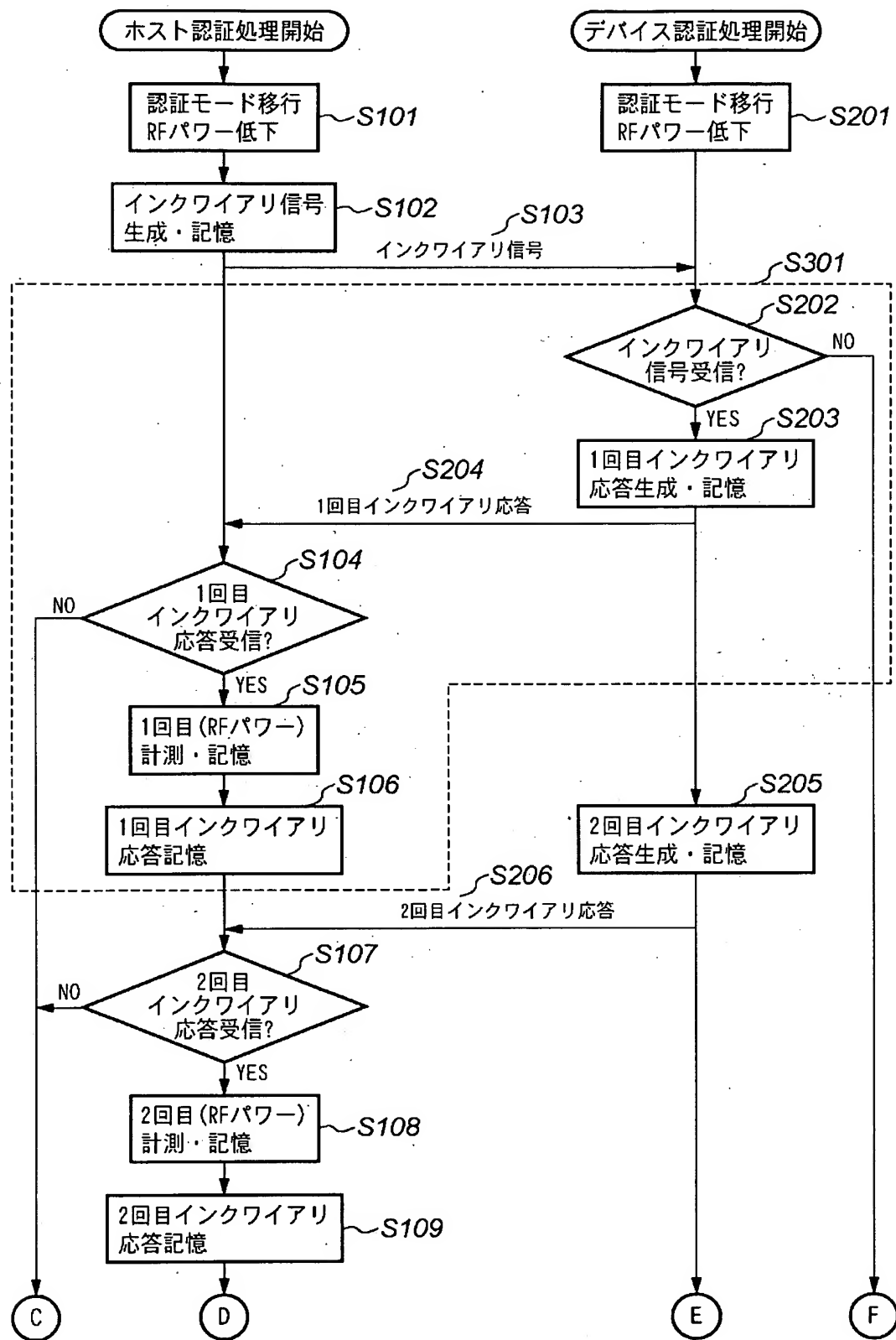
【図 1 2】



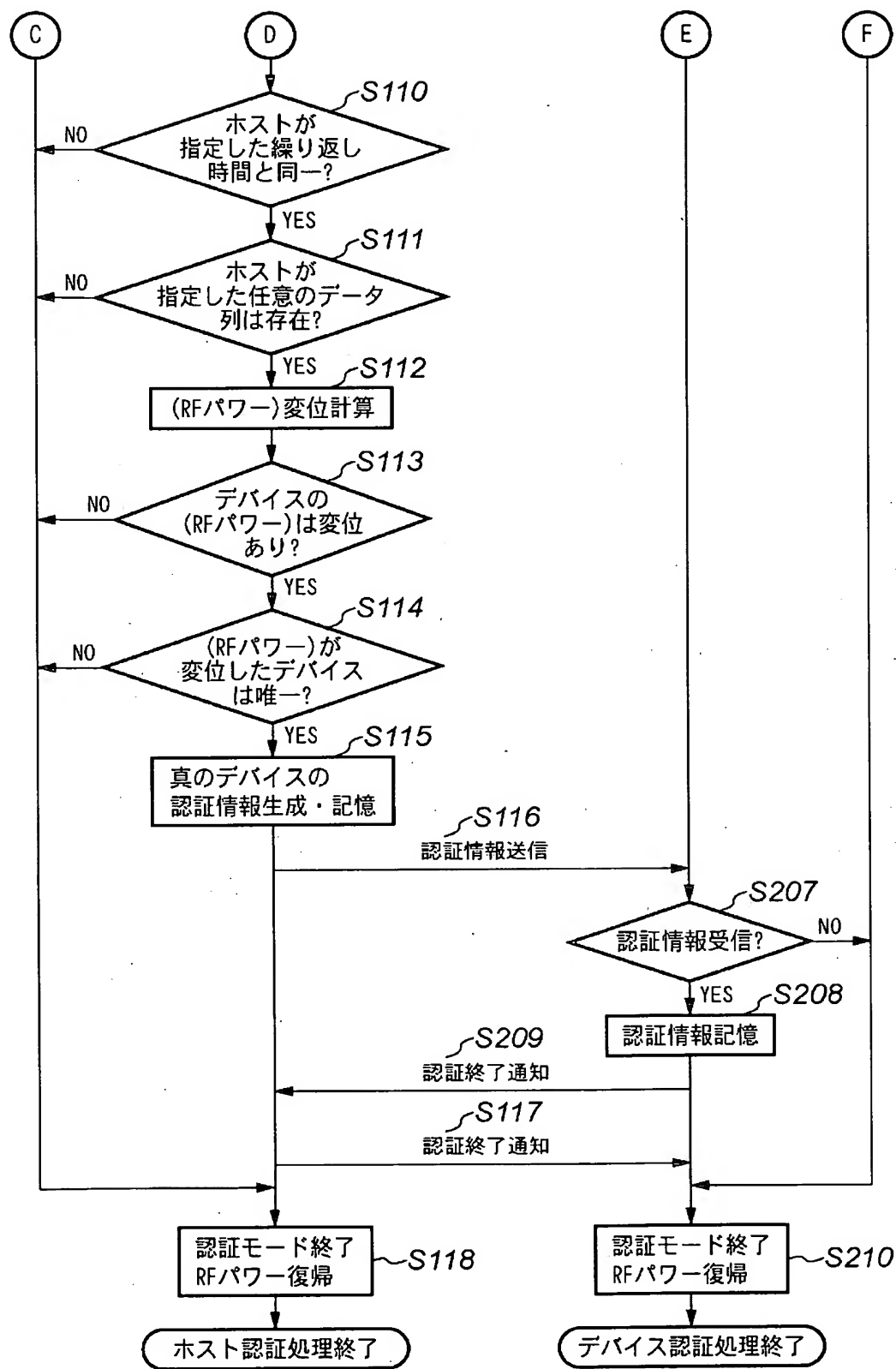
【図13】



【図14A】



【図 1 4 B】



【書類名】 要約書

【要約】

【課題】 操作者にかかる作業を簡便なものとし、且つ、それぞれの装置が単一の無線通信手段を利用しながらも、二者間の認証処理を行えるようになる。

【解決手段】 認証開始指示ボタンが操作されると、ホスト装置は、自身のRFパワーを下げ、通信可能距離を数十センチメートル程度にする(S101)。そして、ホストは、照合データと時間間隔データを内包するインクワイアリ信号を発信する(S103)。このインクワイアリ信号を受信できたデバイスは、照合データと自身を特定する情報を内包したインクワイアリ応答信号を、指示された時間間隔で送信する。ホストは、このインクワイアリ応答が設定された時間間隔で受信され(S110)、照合データを含み(S111)、受信信号強度が所定範囲の変化があり(S113)、尚且つ、インクワイアリ応答が唯一のデバイスからものである場合(S114)に限って、認証情報を送信する(S116)。

【選択図】 図10A

出願人履歴

0 0 0 0 0 1 0 0 7

19900830

新規登録

5 9 5 0 1 7 8 5 0

東京都大田区下丸子3丁目30番2号

キャノン株式会社